AD-A260 785

Computer-aided Acquisition and Logistic Support: Rights in Technical Data

PL018R1

William Garrett Stewart II
Philip W. Clark

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

DTIC
ELECTE
FEB 24 1993
S B D

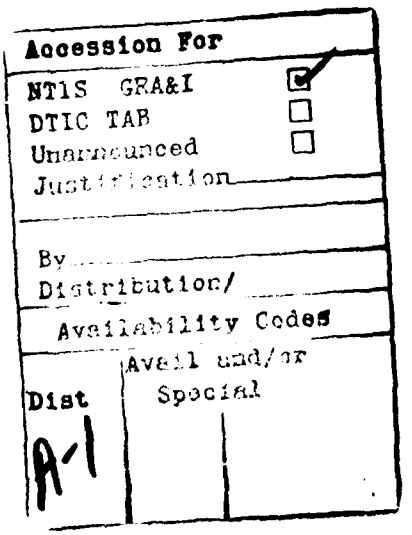
93-03832

February 1992

Computer-aided Acquisition and Logistic Support: Rights in Technical Data

PL018R1

DTIC QUALITY INSPECTED 3



William Garrett Stewart II
Philip W. Clark

Prepared pursuant to Department of Defense Contract MDA903-90-C-0006. The views expressed here are those of the Logistics Management Institute at the time of issue but not necessarily those of the Department of Defense. Permission to quote or reproduce any part except for Government purposes must be obtained from the Logistics Management Institute.

Logistics Management Institute
6400 Goldsboro Road
Bethesda, Maryland 20817-5886

REPORT DOCUMENTATION PAGE

Form Approved
OPM No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources gathering, and maintaining the data needed, and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, DC 20503.

1. AGENCY USE ONLY *(Leave Blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	Feb 92	Final

4. TITLE AND SUBTITLE
Computer-aided Acquisition and Logistic Support: Rights in Technical Data

5. FUNDING NUMBERS
C MDA903-90-C-0006
PE 0902198D

6. AUTHOR(S)
William G. Stewart II and Philip W. Clark

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Logistics Management Institute
6400 Goldsboro Road
Bethesda, MD 20817-5886

8. PERFORMING ORGANIZATION REPORT NUMBER
LMI-PL018R1

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Major General Edward R. Baldwin
Director, CALS Policy Office
Room 3D833, The Pentagon
Washington, DC 20301

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
A: Approved for public release; distribution unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

The Department of Defense is currently implementing the Computer-aided Acquisition and Logistic Support (CALS) concept of electronic exchange of computer-readable technical data between DoD and its contractors. Contractors have expressed concerns about the security of their sensitive data under the new CALS concept. LMI identifies significant contractor concerns and proposes possible solutions for further development. One set of alternative remedies specifically addresses issues of data security under the CALS concept. For example, LMI proposes that data be delivered into a discrete data base, rather than permitting authorized users to access contractors' corporate data bases. However, the issues of CALS data security are intimately connected to more longstanding issues of what data contractors must deliver to DoD and what uses DoD may make of delivered data. Therefore, LMI also proposes a set of possible solutions to these issues.

14. SUBJECT TERMS
Computer-aided Acquisition and Logistic Support; CALS; Rights in technical data; Technical data; Competition; Industrial base attrition; Industrial base; Technical data security; Spare parts; Major systems

15. NUMBER OF PAGES
131

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	18. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

Executive Summary

COMPUTER-AIDED ACQUISITION AND LOGISTIC SUPPORT: RIGHTS IN TECHNICAL DATA

When DoD contracts with a supplier to buy a product, or to have a product developed, the contract calls for delivery of some amount of information needed to install, use, maintain, and support the product. Such information is known as "technical data."

In the past, technical data have been delivered primarily in paper form (or equivalent microfilm images), often running to thousands of pages for major items. Now, however, DoD is implementing the Computer-aided Acquisition and Logistic Support (CALS) concept of computerized delivery and use of technical data. CALS has the potential for delivering great benefits to DoD. But there are serious technical data issues that threaten CALS implementation.

DoD's contract with the supplier specifies how much and what kinds of technical data the supplier must create and deliver to DoD. The contract also determines what uses DoD can make of the data. DoD's contractual right to use technical data for certain broad categories of purposes is known as its "rights in [the] technical data."

Under current contracting rules, the degree of DoD's rights is determined primarily by the source of funding for the development of the product to which the data relate. For example, if the contractor develops the product and the data entirely at its own expense, the data are normally regarded as contractor property, or "proprietary," and DoD would receive only carefully limited rights of use in them. In contrast, with products or data created entirely at Government expense, DoD normally has the right to use the data in whatever way DoD sees fit. But it is often virtually impossible to identify the precise original source of funding or to segregate privately funded technologies from other technologies in the items in which they are incorporated. In such cases, the rights in the technical data are controversial.

DoD and its suppliers have been in conflict for decades over DoD's data rights policies and practices. Above all, contractors strongly protest the taking of what they regard as their proprietary design and manufacturing data. Design and manufacturing data contain detailed information about the product, the manufacturing processes, and the underlying technologies. If exposed to a supplier's competitors or potential competitors, such data enable these other suppliers to make the product or commercially exploit the technology and thus capture some of the company's market, with adverse financial consequences to the company.

The position of DoD has been that it needs design and manufacturing data to (1) establish alternative manufacturing sources, (2) ensure sources of supply if the original contractor can no longer perform, and (3) meet emergency repair and overhaul situations. DoD establishes alternative manufacturing sources to protect itself from being totally dependent on the original supplier, with the possibility that the original supplier may exploit its monopoly position to charge DoD exorbitant prices for its product. In addition, DoD believes it needs additional sources of supply to respond to sudden demands for increased production ("surge") to meet national emergencies such as the Persian Gulf War.

The introduction of CALS complicates these data rights conflicts. CALS is being implemented in two phases. Phase I, focusing on developing standards for exchanging computer-readable data, has received strong industry support. But many DoD contractors are greatly concerned about Phase II. The Phase II concept calls for DoD and other authorized users to have direct computer access to a portion of each weapon system contractor's corporate technical data base. This concept has raised widespread contractor fears that (1) unauthorized users may improperly gain access to the network, (2) users may be able to gain unauthorized access into areas of the corporate data base that should be "off limits" to noncompany personnel, and (3) users may be able to accumulate enough nonsensitive information to derive corporate technical secrets, especially with the help of the enhanced analytical power of the computer. *In other words, contractors fear that CALS will make possible the de facto delivery of sensitive data, regardless of what their contract with DoD might require.*

To maximize benefits of CALS and to meet these legitimate objections, we recommend that DoD revise current plans for implementing CALS Phase II, and instead provide for

- An autonomous data base for integrated weapon system data, separate from the contractor's corporate data base
- Incremental implementation, with more sensitive data added into the data bases as security is proven
- Multisite log-ins, with requests for access to data residing in multiple locations instantly forwarded to all sites containing the requested data.

By themselves, however, these changes are not enough. Any CALS-type integrated data base system by its very nature will present greatly increased opportunities for exposure of contractor-developed data to other system users, in comparison with the current system of paper documents stored in Government repositories where physical access can be tightly controlled. Imposing security controls as stringent as those used in a classified national security network would stifle the accessibility and rapid exchange of data that are the whole purpose of CALS. As long as contractors are required to deliver data that they regard as vital to their economic health into a computer-based system allowing widespread access by potential competitors, they will regard that system as inherently threatening to their vital interests. Thus, unless the longstanding conflicts over DoD technical data policies requiring delivery of sensitive contractor data are satisfactorily addressed, contractors will not fully support a CALS-type system. DoD technical data policy and CALS data security issues must *both* be satisfactorily addressed before CALS implementation can proceed with a high degree of industry support and cooperation.

From the contractors' perspective, the only truly satisfactory solution would be for DoD not to require contractors to deliver design and manufacturing data containing any proprietary information, whether into a paper repository or a computerized data base. But from DoD's perspective, that solution would make sense only if (1) the justifications for DoD's use of such data are invalid, (2) the liabilities of the policy outweigh the potential benefits, or (3) there are alternatives that would meet DoD's critical needs without the liabilities. There is good evidence suggesting that both (1) and (2) may be the case, and we believe that there are viable alternatives to DoD's current data rights policies and practices that should be explored.

Accordingly, we recommend that DoD consider the following:

- Abandoning the routine use of competition for re-producing systems, components, and complex spare parts and instead incorporating price competition for spares as part of the overall production contract with the original source.
- Permitting contractor nondelivery of proprietary design and manufacturing data, with protection for DoD through third-party escrow of the data or "march-in" rights to contractor-stored data.
- When subsequent spares or component pricing by the original supplier is regarded by DoD as unreasonable, resolving the pricing dispute first with an independent third-party arbitrator before establishing alternative sources.
- Revising the Defense FAR (Federal Acquisition Regulation) Supplement rights in technical data rules
  - To clarify rights in the products of R&D
  - To permit contractor delivery of only form, fit, and function data when the data are created at private expense or – if alternative sourcing is abandoned and escrowing adopted – to permit it regardless of DoD rights in the data, except in those rare cases when alternative sources *must* be created (as when the original contractor cannot meet surge requirements) and direct licensing of new sources is not possible.
- Clarifying the delivery requirements of its specification for technical data, MIL-T-31000.

CONTENTS

CONTENTS (Continued)

CHAPTER 1

OVERVIEW

BACKGROUND

When DoD contracts with a company to buy a product, or to have a product developed, it usually also contracts for some amount of technical information needed to install, use, maintain, and support the product, among other things. This technical information is known as "technical data." As used in Government contracting, technical data must be recorded in some form (such as engineering drawings, written reports, manuals, phonograph records, photographs, movies, compact disks, or computer tapes). The term does not embrace computer software or financial administration and management information.

In addition to the various physical forms the technical data may take, the data may also vary in the degree of technical detail they reveal about the product. Technical data that contain enough detail about a product so that another competent manufacturer could manufacture an essentially identical product are referred to as "product drawings," "detailed data," "detailed design data," or simply "design data." The terms "manufacturing data" and "manufacturing process data" refer to all the information about production and assembly processes and techniques necessary to manufacture the product. An example of a less detailed category of data would be "form, fit, and function data," which would give enough product detail to permit someone to identify physically and functionally interchangeable (but not necessarily identical) products. And manuals for installation and repair would also have much less product detail than would design and manufacturing data.

The contract between the company and DoD determines how much technical data the company will create and deliver to DoD – and in what detail and in what form the data will be. The contract also determines what uses DoD can make of the data. The contractual right for DoD to use technical data for certain broad categories of purposes is known as its "rights in [the] technical data."

These rights are not the same as "ownership." The concept of ownership is a murky one at best when it comes to Government contracts involving technical data,

since there is no formal, legal title in the technical data, as there might be in other kinds of property. Today, the most commonly held concept of ownership has to do with who paid for developing the data. A contractor that, entirely on its own, funds all of the development of an item, part, component, or process usually considers the technical data associated with that "new" product or process to be its own property. The contractor will commonly refer to such data as its "proprietary" data. Similarly, when the Government provides all of the funding for developing a product or process, the Government's agents generally think of the associated technical data as rightfully "belonging to" or being the property of the Government. When both parties contribute some value – especially when both contribute some of the development funds or when proprietary components are incorporated into a larger item – the ownership issues become confused and often controversial. It must be emphasized that these ideas of ownership are popular sentiments, not necessarily legal principles.

In its entire history prior to World War II, the United States had never had a large, permanent industry dedicated to supporting the professional Army and Navy. When the Military Services needed equipment, they either bought commercial products, designed and developed equipment themselves and then contracted with private companies to manufacture it, or built the items in Government arsenals. Issues of ownership of technical data were nonexistent, because the source of funding and the locus of the effort to create new technologies and products were either clearly private or clearly Government.

But at the end of World War II, a new industry began to emerge; it consisted of companies selling primarily or exclusively to the military and participating directly in the entire design, development, and production process for weapon systems. These defense companies began to incorporate in their weapon designs and development some of their own privately developed technologies. This incorporation of contractors' proprietary technical data into military weapon systems set the stage for the conflicts over rights in the technical data that have emerged in recent years.

Those conflicts were not triggered, however, until DoD began to use contractors' proprietary technical data to set up new sources of manufacturing in competition with the original supplier, with the goal of reducing prices by this competition.

Alternative sources were established for systems themselves and for their components and parts.

Contractors regarded this new practice as threatening their vital interests. For one thing, the establishment of alternative suppliers, by whatever means and for whatever reasons, obviously took defense business directly away from the original supplier. For another, DoD sometimes would give contractor-developed design and manufacturing data to the new alternative sources of supply, as the most effective way to enable them to manufacture the product. Thus, DoD exposed sensitive data to the contractor's competitors and potential competitors. The data were sensitive precisely because they documented all the details of the manufacturer's products, processes, and underlying technologies and thus could enable someone else to produce an identical or competitive product or otherwise exploit the technology revealed in the data. In other words, DoD's practice not only reduced the contractor's immediate defense business by setting up alternative suppliers, it threatened all of the contractor's business derived from that product or technology.

This economic threat was especially acute for certain companies. First, it threatened subcontractors more than it did prime contractors. The major prime contractors were primarily integrators of the work of others – the subcontractors. Most of the technological composition of weapon systems came from the subcontractors, and the prime contractors generally had relatively little of their own proprietary, sensitive data at risk. Second, for some companies – again, usually subcontractors – the danger of data exposure was especially acute because their whole business depended on one or a few products, processes, or technologies; loss of their markets in those products or processes could wipe them out. Third, companies selling high-technology products were greatly at risk. Such products required heavy investments in R&D and experienced very short effective product lives, because of the increasingly rapid obsolescence of technology. The only way such products could be economically viable was if the company were to control a very high market share for the product's short life. Exposing the underlying technical data to competitors threatened that market control. Fourth and finally, companies selling the products – or products derived from technology exposed in the technical data – in the commercial marketplace as well as to DoD were seriously threatened by DoD's practice, because the amount of potential loss to competitors was greatly increased.

For a more complete discussion of the economic and business factors behind technical data issues, see Chapter 4.

In the 1980s, two major developments strongly influenced DoD's policies and practices concerning technical data. The first of these was a legislatively driven heightened emphasis on competition; the second – to be discussed later – was the initiation of the Computer-aided Acquisition and Logistic Support (CALS) concept.

With regard to the first, in reaction to scandals over the prices DoD was paying for spare parts and common items, Congress passed a number of laws emphasizing competition during the entire weapon system life cycle, from development through production and support. As a result, DoD adopted policies and contracting practices that aggressively sought to develop competitive alternative sources for weapon systems, components, and spare parts in the belief that competition would significantly reduce the prices DoD would have to pay for the items. Although this was not the first time DoD had attempted to implement such competition, the effort was now greatly intensified. For a more comprehensive discussion of these laws and of the evolution of the technical data rights policies and issues, see Chapter 2 and Appendix A.

Although price reduction was the primary justification for obtaining competition through alternative sourcing, another reason often cited during the 1980s was the belief that DoD needs many potential sources of supply in order to respond to demands for increased production in national emergencies. These sudden demands for increases in production are known as (1) "surge" requirements, for short-term national security events (such as the Persian Gulf War), and (2) "mobilization" requirements, for events on the scale of a world war.

Regarding the use of contractors' detailed design and manufacturing data, DoD cites two needs for the data, besides the need to have the data in order to establish alternative sources of supply. First, DoD declares that it needs the data in order to guarantee a source of supply if the original contractor can no longer perform, or refuses to continue to perform, the contract. Second, DoD cites the need to perform emergency major overhaul and repair of systems such as ships, which may require the use of the system's detailed design or manufacturing data. See the further discussion in Chapters 2 and 5.

The other major 1980s development mentioned above – CALS – involves computerized development, delivery, and use of weapon system technical data. The CALS concept is in large part a response to developments in industry [such as concurrent engineering, computer-aided design (CAD), and computer-aided manufacturing (CAM)] that have made it possible to design and build products using the powerful resources of the computer. The goal of CALS is to harness this power in developing, producing, and supporting weapon systems.

CALS is to be implemented in two carefully managed stages. Phase I of CALS, covering the period from inception of the program in the mid-1980s through 1992, has focused on the development of standards that will govern the electronic exchange between DoD and its contractors of computer-readable ("digital") technical data. Emphasis has been on improving data transmission rather than on the content of the data being delivered. The only real difference between Phase I and the prior system is in the form of the data: computer-readable tape or optical disk rather than paper or microfilm.

This means that issues of data security and control are not radically different under CALS Phase I from what they were before. The contractor still controls the content of the data being delivered to DoD and the destination of the data. Data can still receive corporate review and approval before release. Disputes over the quality, quantity, and type of data and the rights in the data can be resolved before final delivery and acceptance. Because CALS Phase I does not significantly change contractor control over technical data, it has enjoyed a high degree of industry support.

CALS Phase II is a different story. Upcoming plans for it have evoked strong contractor concern. That is because the Phase II concept calls for integrated computerized networks (the Integrated Weapon System Data Base, or IWSDB) embracing all technical data related to weapon systems. Contractors will produce the technical data within their own corporate data bases, and all the technical data relating to a weapon system will reside at the various contractor locations, under a concept known as the Contractor Integrated Technical Information Service (CITIS) contract. Instead of physical delivery of technical data, DoD and all other authorized users will have direct and immediate access to an agreed-upon portion of the contractor's data base, using individual computer workstations.

These Phase II features introduce a radically different environment for data security and control. First, control over access to the system (and thus to sensitive contractor data) will become more subject to error. In the paper system, a requester of technical data has to "log in" separately to each repository or data base containing technical data the requester needs. But in CALS Phase II, there would be only one log-in, to the entire system. If approved, the requester would then instantly gain access to all data requested. The multiple checks against unauthorized access would now be replaced by only one, with consequent multiplication of probability of mistakes and of the potential for unauthorized users to gain access to a contractor's sensitive data.

Second, the danger of unauthorized access to areas of the contractor's internal corporate data base technically not subject to external exposure would be greatly increased. That is because internal security controls within the CALS network must allow for quick, easy access; they would therefore be easier to defeat (by someone already in the network) than would controls aimed at keeping unauthorized persons entirely out of the network itself. In other words, it would be easier for a competitor who has gained access (even if legitimate) to the system to penetrate another contractor's sensitive data repository – to which the competitor does not have authorized access – than it would otherwise be.

Third, even if a competitor did not specifically attempt to gain unauthorized access to a contractor's sensitive data, the competitor could take advantage of the integrated data base capabilities to "browse" through various accessible parts of the contractor's data and accumulate enough nonsensitive information to derive sensitive information, a phenomenon known as "aggregation." This potential is enhanced by the capabilities of the computer itself, which enable a user to process and analyze vast quantities of information in a way not possible with volumes of paper documents.

All of these contractor concerns essentially amount to fears that implementation of CALS Phase II – as presently conceived – will produce de facto delivery of contractors' sensitive data even if delivery of the data is not legally required under the contractor's development or production contract. The concerns thus add to, and intensify, the already existing conflicts between DoD and its

contractors over what data should be deliverable to DoD and what uses DoD should be able to make of the data.

Underlying technical data conflicts and CALS data security issues are intimately related, because each must be satisfactorily addressed in order to win the support of industry necessary for CALS implementation. Before contractors will enthusiastically support any technical data system (CALS or otherwise), concerns over the required delivery of sensitive contractor data and over DoD uses of the data must be overcome to the extent that contractors will not feel that their vital economic interests are being threatened. On the other hand, even if DoD technical data policy were to be altered to the satisfaction of contractors, nothing would be gained if CALS implementation then threatened to undo that policy through technological processes. To repeat, DoD technical data policy and CALS data security issues must both be satisfactorily addressed before CALS implementation can proceed with the necessary degree of industry support and cooperation. See Chapter 3 for a more complete discussion of CALS.

FINDINGS AND CONCLUSIONS

Are these conflicts and concerns over technical data issues having an adverse impact on DoD? Yes. As a result of them, some contractors and subcontractors are refusing to provide their best technologies in weapon system development and production programs. Some have refused to participate in key DoD weapon system acquisitions or are dropping out of the defense industry altogether because of technical data concerns. And many industry representatives have indicated that they will not support CALS Phase II as currently conceived, because of the technical data security issues we have noted. As a result of these forms of attrition, DoD weapon systems may be less capable than they could be with the full participation of industry, they may be more expensive because of diminished effective competition, and the CALS program may be jeopardized because of potential lack of cooperation and participation of contractors and subcontractors. For a discussion of the evidence supporting these conclusions, see Chapter 6.

Since the primary justification for using contractors' detailed design and manufacturing data and for establishing alternative sources of supply is to reduce, through competition, the prices DoD pays for items, components, and parts, a principal focus of investigation must be on whether this competition does actually

reduce these prices. As we show in Chapter 7, a body of evidence concludes that competition in production of complex high-technology systems, components, and parts has a high risk of resulting in items that are of lower quality than, or are dissimilar from, the original item, thereby increasing support costs over the system's life cycle. Furthermore, the latest studies of alternative source competition find that it is just as apt to result in higher production prices as in lower ones and that total life-cycle costs are most likely to be significantly higher.

The real issue in pricing is not whether DoD can force the lowest possible price at any particular stage of a weapon system's development and life cycle, but rather whether the price paid by DoD is fair and reasonable, given the underlying economic realities of the business exchange.

With regard to the secondary justification for alternative sourcing, namely surge and mobilization needs, it is not clear that alternative sourcing is necessary. The only circumstance seeming to justify alternative sourcing for surge/mobilization needs would be that in which the original manufacturer cannot provide DoD with a credible plan to meet those needs, should they arise. This should be a rare circumstance, since most manufacturers can hire the required number of additional workers, go to multiple shifts, or build in the necessary excess capacity (at Government expense) at least as well as several smaller sources could. Furthermore, the original source can provide direct licensing arrangements with other potential sources as a means of rapidly expanding production. For a more complete discussion of these findings, see Chapter 7.

RECOMMENDATIONS AND ALTERNATIVE SOLUTIONS

In accordance with the charter for this task, the Logistics Management Institute (LMI) was asked to identify potential areas of solution for the problems and concerns discovered during our investigation. The solutions were meant to be initial identifications for either potential further study and investigation or exploratory development, perhaps with industry participation. For a more complete discussion of the alternatives outlined below, see Chapter 8.

CALS-Specific Alternatives

Recommendation 1: DoD should revise current concepts for implementing CALS Phase II, with possible alternatives indicated below.

Alternative 1. A separate, discrete data base for integrated weapon system data. Instead of the proposed CALS CITIS/IWSDB concept, under which DoD and the contractor would share a portion of each contractor's corporate data base (DoD having access to the data base at the contractor's location), a separate data base could be established for weapon system technical data. Contractors would enter data into this data base only as required under their contracts and only after release of the data has been internally reviewed and approved.

Alternative 2. Incremental implementation. CALS Phase II data bases can be implemented in stages, beginning with a system that incorporates only nonsensitive corporate technical data. As the security of technical data in the system is proved to industry's satisfaction, more sensitive data can then be added to the data bases. The system would grow in step with industry confidence as security measures are demonstrated successfully.

Alternative 3. Multisite log-ins. A possible solution to the concern over improperly granted access to data bases might be to require that requests for access to data residing in multiple locations (as with the CITIS concept) be instantly forwarded to all sites containing the requested level of data. Each CITIS contractor whose data is potentially at risk would have the opportunity to review and challenge the request. Obviously, controls on abuse of this process – such as time limits on the right to challenge – would have to be implemented.

Alternative 4. Multilevel access controls. A common proposal for CALS is to incorporate multilevel access controls similar to those employed in national security classified systems. There are some roughly comparable commercial systems. But there are also grave problems with this concept. First, it is difficult to imagine the CALS concept working as envisioned if classified data are included, since classified systems usually require the kind of tight controls that would prove disabling to CALS. Second, normal personnel turbulence in industry makes it almost impossible to manage the necessary clearances for such a system. Finally, the security controls that would be necessary – even without the inclusion of classified data – would be so inhibiting and perhaps costly that they might preclude the benefits of accessibility that CALS was meant to provide.

Recommendation 2: Once a major system's production contractor has been competitively selected, DoD should abandon the routine use of subsequent re-competition for production of systems, components, and complex spare parts.

The justifications for automatic, invariable use of this practice are weak, while the costs, in price and quality, are extremely high. This is especially true as quantities of production items decrease, as is occurring with declining budgets. Eliminating or radically reducing use of this practice will dramatically improve business relationships with suppliers and enhance DoD's ability to perform its missions, by improving the quality and breadth of the industrial base of suppliers offering their best capabilities in DoD weapon systems programs.

Recommendation 3: DoD should incorporate price competition for spare parts as part of the overall production contract with the original source.

If price competition must be the measure of price reasonableness, then if it is used at this earlier stage of the acquisition cycle, the results can be cited to demonstrate price reasonableness while not violating the contractor's vital interest in protecting its sensitive technical data. Alternatives include the following:

Alternative 1. Extensive initial provisioning. DoD fields its systems with an initial stock of spare parts. One alternative to competition for follow-on buys of spare parts would be greater one-time, up-front procurements of parts stocks sufficient to support the system well into its projected life, competed as part of the production contract competition.

Alternative 2. A production contract with a long period of contractor support. In this case, the base contract would include a commitment by the contractor to support the item for a fixed number of years. The Army negotiated such a contract, with 15 years of contractor support, for its mobile subscriber equipment program (mobile phones). Award would again be based on the best total package offered. And, again, DoD would get replacement parts support at a price based on open competition, while the contractor would be able to keep its sensitive data.

Alternative 3. A production contract with a fixed period of spares pricing, followed by contractor option. In this case, offerors would include a price for spares for

a fixed number of years, perhaps with annual adjustments for inflation or other relevant factors, as part of the production contract proposal. Technical data sufficient to establish alternative sources would be placed in escrow. At the expiration of the initial support period, continued spares support prices could be renegotiated. A host of potential arrangements could be devised as variants of this alternative, such as mandatory arbitration, guaranteed right of DoD access to escrowed data in the event of failure to agree on prices or contractor nonperformance, or direct contractor licensing of alternative sources.

Recommendation 4: DoD should consider adopting a policy of permitting contractor nondelivery of proprietary, sensitive technical data, with protection to DoD through third-party escrow of the data or else "march-in" rights to contractor-stored data.

As noted, DoD's reason for requiring contractors' design and manufacturing data is mainly to establish additional sources of supply, in order to introduce price competition and thereby reduce prices. Also as noted, a secondary reason is to provide for surge and mobilization needs. We have recommended that the practice of routine alternative sourcing be generally abandoned. That would leave only two secondary purposes in demanding delivery of these categories of detailed data: security of supply and facilitating emergency repair and overhaul.

Fulfillment of these two purposes does not require physical delivery by the contractor and physical possession of the data by DoD. What is required is that DoD have guaranteed access to and use of the data when the actual need occurs. This requirement can be met by having the contractor deliver the data into a third-party escrow, with DoD having the right of inspection to guarantee that the data are current, complete, and fit for the intended purpose. DoD would need the right to take possession of the data upon the occurrence of certain stipulated events. A variation would be to allow the data to reside with the contractor, but isolated from routine DoD access, with march-in rights for DoD to have access under the named conditions.

If alternative sourcing is not pursued, and if security of supply and emergency repair needs are protected through escrow provisions, there is no reason for DoD to require delivery of design and manufacturing data, regardless of who funded their development or what rights DoD has in them.

Recommendation 5: DoD should consider adopting a policy of seeking independent third-party arbitration for price reasonableness determinations before establishing alternative sources.

Recommendation 6: DoD should revise the Defense FAR (Federal Acquisition Regulation) Supplement (DFARS) rights in technical data rules.

Revision 1. Clarifying rights in the products of R&D. The current DoD acquisition regulations give DoD unlimited rights (that is, the right to do anything it wants with the data) in the technical data resulting from all R&D work. However, there is a very significant difference between (1) R&D that is conducted solely for the purpose of increasing knowledge and the nation's technological base and (2) R&D that has as its purpose the eventual or potential development of a product for DoD inventory. The regulations, the standard contract clauses, and the contracts themselves should be revised to distinguish clearly between these two types of effort and to provide for a different level of DoD rights accordingly.

Revision 2. Contractor nondelivery of sensitive data. At a minimum, in consonance with the discussion in Recommendation 4 above and even without adoption of Recommendation 2, the DFARS should be revised to permit delivery of only form, fit, and function data when the data are created at private expense. If Recommendations 2 and 4 are both adopted, the DFARS should be revised also to permit delivery of only form, fit, and function data regardless of DoD rights in the data, except in those rare cases when alternative sources must be created (as when the original contractor cannot meet surge requirements) and direct licensing of new sources is not possible. If Recommendation 4 is adopted, contract clauses and policy guidelines should be developed to permit use of escrow and march-in rights.

Recommendation 7: DoD should clarify the delivery requirements of its specification for technical data, MIL-T-31000.

The current version of this specification is not clear about certain points that are very critical to industry. Although the specification's data item description (DID) for product drawings indicates that only form, fit, and function data need be delivered for limited rights items, the language and its operation with other parts of the document are ambiguous. It is not clear whether this nondelivery provision is mandatory for the Government. (See the discussion in Chapter 8.) We recommend

that the ambiguity be eliminated and that the requirements be revised in accordance with the above recommendations.

CHAPTER 2

DEPARTMENT OF DEFENSE TECHNICAL DATA POLICIES

INTRODUCTION

In order to understand industry's major concerns regarding CALS implementation, it is necessary to understand some of the basic policy concepts governing DoD's acquisition and use of technical data. This chapter reviews those concepts and their underlying rationales. Since CALS will primarily incorporate information on weapon systems rather than on other products bought by DoD, the emphasis here and throughout the rest of this report will be on technical data relating to weapon systems.

Contracting for products and services is regulated by a host of laws, regulations, and policy documents. Contracting for technical data is no exception. The process of determining what technical data the contractor will deliver – and what rights the Government will have in the data – is governed by numerous statutes, regulations, and DoD policy documents. Before reviewing DoD's policies controlling the buying of technical data, it is helpful to look at their evolution.

BRIEF HISTORY OF DoD TECHNICAL DATA POLICY

As noted in Chapter 1, the United States had never had a large standing peacetime Army and Navy until after World War II. Neither did it have a large industry dedicated to supporting the professional Army and Navy. The Military Services either bought commercial equipment for their needs or designed military items themselves (in-house) and then either built the items in Government arsenals or merely contracted for their manufacture. Conflicts and issues about rights in technical data did not arise [1].

Just before and during World War II, that situation began to change. Private firms began large-scale participation in the design and development of weapon systems. These private firms began to claim proprietary interests in some designs,

components, and manufacturing processes incorporated in the weapon systems they helped build.

After the war, the United States accepted a vast global responsibility and the requirement for a large, committed force to go with it. With that radical historical change, a defense industry – consisting of corporations selling primarily or exclusively to the military and participating directly and intimately in the entire design, development, and production processes – began to emerge.

Yet, even with the advent of private-company proprietary claims, there were no serious conflicts over rights in technical data in the early years following World War II. That was principally because the Military Services did not make any use of their contractors' technical data – such as providing the contractor-developed data to other manufacturers – that could threaten the contractors' vital economic interests. The Military Services, combined into DoD in 1947, simply bought all their equipment from the original supplier and allowed prime contractors to do the same with their own vendors. In addition, at least through the end of the Korean War, defense contractors were working to capacity and thus were not seriously concerned about alternative sources of supply for their equipment. There was enough business to go around [1].

After the Korean War, however, the cost and complexity of systems soared. Critics in Congress and elsewhere focused on DoD sole-source procurements as a primary cause of high costs. They believed that increased competition for the production of systems, components, and parts would help reduce those costs. As a result, DoD adopted a number of policies and practices to increase competition and control costs. One of these practices was the "breakout" of equipment for "competitive reprocurement." In competitive reprocurement, DoD took the technical data of an initial contractor and distributed the data to other potential manufacturers to permit them to bid for subsequent production of the equipment, especially parts. Using this procedure created alternative sources of supply and introduced price competition for all subsequent purchases.

The practice of providing an original manufacturer's technical data to other suppliers brought DoD into conflict with many of its contractors and subcontractors. These suppliers protested that their own proprietary data were being given to their competitors, with disastrous consequences for their own economic interests.

DoD attempted to resolve this conflict, and to accommodate contractors' concerns, with several revisions to its regulations governing contracting for technical data. In one of these revisions, DoD adopted the policy of allowing contractors to withhold any proprietary data not specifically required by the contract. The contractor was basically allowed to determine what was proprietary. But many contractors responded by withholding all data even remotely tinged with a proprietary claim. Some would substitute their own specifications for more standard ones, or their own designs for ones in which DoD had unlimited rights, and then claim proprietary rights and withhold the data. As a partial result, the data held by DoD deteriorated to the point that they could not be used effectively for maintenance, repair, overhaul, stockpiling, and DoD's numerous operational needs. Many in DoD concluded that contractors could not be entrusted with the determination of what data they would deliver [1].

In the 1980s, as the United States began to invest heavily in a rapid defense buildup, critics of the buildup itself and of the manner in which it was being conducted began surfacing one "horror story" after another about overpriced hammers, diodes, Allen wrenches, coffee pots, toilet seat covers, and other spare parts and common items. Congress and the public were incensed. The problem, once again, according to congressional critics, was that DoD was buying too much from sole-source suppliers. The solution, these critics were certain, was more competition at every stage and phase of Defense procurement. They were also concerned that one of the main reasons why DoD was not competing its spare parts acquisitions more was that it was not receiving the necessary rights in technical data. In addition, small businesses repeatedly testified that they were being cut out of defense parts procurements because DoD lacked the technical data needed to manufacture the parts [2].

In response to this situation, Congress passed two key statutes in 1984. The first of these was the Competition in Contracting Act of 1984 (CICA) [Public Law (P.L.) 98-369], which mandated "full and open competition" in all Federal procurements, with only seven narrow exceptions permitted. Approval to use the exceptions was made difficult.

The Defense Procurement Reform Act of 1984 (P.L. 98-525), passed 3 months later, had the specific intent of dealing with alleged excessive prices for DoD's replenishment (spare) parts. As with CICA, the Reform Act emphasized competition,

but it further focused on rights in technical data, requiring that, in both development and production contract solicitations for major systems, DoD consider requiring offerors to give DoD the rights necessary to reprocure spare parts from other sources [3].

The Reform Act was later amended, after industry objections, and now *prohibits* DoD from requiring contractors, as a condition of doing business with DoD, to relinquish their rights in technical data that would enable DoD to reprocure the item competitively. The Reform Act permits two exceptions: (1) When DoD determines that the original supplier will be unable to satisfy program schedule or delivery requirements or (2) when the original supplier does not satisfy DoD that it can meet mobilization requirements.

The Reform Act also established an elaborate set of procedures for challenging and validating contractor claims in technical data. Other changes to the law now require negotiations between the contractor and DoD to determine data rights when both parties have contributed funds in developing an item or process.

Having dealt with the spare parts issue, Congress next focused its attention on the major weapon systems themselves. In 1985, Congress passed P.L. 99-145, requiring that all major systems acquisitions provide for competitive alternative sources for the system and each major subsystem from the beginning of full-scale development *through the end of production.* Exceptions were provided if the Secretary of Defense determined, for example, that alternative sourcing would produce unacceptable costs or delays or would be adverse to national security interests. But if an exception was exercised for a particular program, the Secretary was required to report this fact, with detailed justifications, to Congress. In the FY91 DoD Authorization Act, this section of the U.S. Code (10 U.S.C. 2438, formerly 2305a) was substantially amended to eliminate the presumption in favor of alternative sourcing for major systems and the onerous reporting requirements. The law now requires only that major system acquisition strategies include the *option* of alternative sourcing, if that would reduce risk or cost or would result in improved design without undue delay or adverse national security consequences (P.L. 101-510, Section 805).

DoD responded to these and other statutory requirements with a series of regulation changes. The most recent such change was published as an interim rule in October 1988 and remains in effect today.

DoD TECHNICAL DATA POLICY TODAY

As we have noted, policies concerning technical data are contained in a number of DoD regulations (such as the interim rule mentioned above), instructions, directives, and other documents. With regard to the conflicts over technical data between DoD and its contractors, three of these policy documents – a regulation, an instruction, and a specification – are key; this section will focus on them.

The standard clauses used in Government contracts to govern rights in technical data, and the instructions on when and how to use those clauses, are contained in the FAR and in the DFARS. The FAR is a Government-wide regulation that replaced the Defense Acquisition Regulation (formerly the Armed Services Procurement Regulation) and its civil agency counterpart, the Federal Procurement Regulations, in 1984. Each agency may supplement the FAR with its own specific rules, as long as they do not conflict with the FAR. The DFARS is DoD's agency regulation under the FAR.

The brief, general technical data policy statement in the FAR applies to all Federal agencies, including DoD. However, the remainder of the FAR data rights rules and clauses apply only to the civil agencies. Except for that minimal introductory FAR policy statement, DoD is governed solely by its own regulations regarding data rights.

The DFARS October 1988 Technical Data Interim Rule

Department of Defense general policies and procedures relating to the acquisition of technical data, as well as the rights in technical data, are found in DFARS Subpart 227.4. The current version of that regulation is the interim rule of October 1988. The standard contract clauses implementing the policies in that subpart are found in DFARS 252.227-7013 through 7037 (a total of 19 clauses, since some of the numbered clauses are reserved).

Acquiring Data and Rights in Data – Balancing the Interests

Subpart 227.4 begins with a discussion of the need to balance the sometimes competing interests of the contractor and the Government in acquiring technical data and rights in technical data, as follows:

> (a) *The Government's Interests.* The Government has extensive needs for many kinds of technical data and the rights to use such data. Its needs may exceed those of private commercial customers. Millions of separate items must be acquired, operated and maintained for defense purposes often at points remote from the source of supply. Technical data are required for training of personnel, overhaul and repair, cataloging, standardization, inspection and quality control, packaging and logistics operations. Technical data resulting from research and development and production contracts must be disseminated to many different users. The Government must make technical data widely available to increase competition, lower costs and provide for mobilization. Finally, the Government has an interest in encouraging contractors to develop new technologies and to improve existing technologies to satisfy Government and commercial needs. To encourage contractors and subcontractors to expend resources in developing applications of these technologies, it may be appropriate to allow them to exclusively exploit the technology.
>
> (b) *The Contractor's Interests.* Commercial and nonprofit organizations have property rights and economic interests in technical data. Technical data are often closely held in the commercial sector because their disclosure to competitors could jeopardize the contractor's competitive advantage. Public disclosure can cause serious economic hardship to the originating company.
>
> (c) *The Balancing of Interests.*
>
> (1) The Government's need for technical data and a contractor's economic interest in it do not necessarily coincide. However, they may coincide. This is true in the case of innovative contractors who can best be encouraged to develop items of military usefulness when their rights in such items are scrupulously protected.
>
> (2) The Government needs to encourage delivery of data essential for military needs, even though that data would not customarily be disclosed in commercial practice. When the Government pays for research and development, it has an obligation to foster technological progress through wide dissemination of the information and, where practicable, to provide competitive opportunities for other interested parties.
>
> (3) Acquiring, maintaining, storing, retrieving, protecting and distributing technical data are costly and burdensome for the Government. Therefore, it is necessary to avoid acquisition of unnecessary technical data.

Buying Only Minimum Essential Needs

The regulation goes on to say that

> The Department of Defense shall obtain only the minimum essential technical data and data rights.... In deciding how to acquire data and data rights, the Department of Defense will use the least intrusive procedures in order to protect the contractor's economic interests.

And with regard to commercial items, the regulation states that DoD will

> ...limit acquisition of technical data and rights in technical data pertaining to commercial items developed at private expense; neither data nor data rights should be acquired for the competitive acquisition of such a commercial item.... DoD will normally only obtain technical data and data rights... such as those needed for operation, maintenance, installation, and training.

The regulation requires high-level approval for a contracting officer to acquire more data or data rights than these for commercial items.

Rights in Technical Data

The regulation provides for three basic categories of DoD rights in the technical data delivered under a contract:

- *Unlimited rights.* These give DoD the right to use, duplicate, or disclose the technical data in any way, for any purpose, to anyone or to the whole world.
- *Government purpose license rights (GPLR).* These are royalty-free rights to use, duplicate, and disclose data for Government purposes only and to permit others to do so for Government purposes. The principal difference between these rights and unlimited rights is that the contractor that developed the data retains the exclusive right to commercialize the data (develop the item or process and sell it in a commercial market). This means, of course, that as is not the case with unlimited rights – the Government cannot publish the data in any public forum for the benefit of general knowledge. But DoD can give the data to other potential makers of the product in order to establish additional sources of supply. When the data are given to such suppliers, they must agree not to use the data for commercial purposes.
- *Limited rights.* These give DoD the right to use the data for internal Government purposes only (these purposes do not include manufacturing). Without the written permission of the contractor or subcontractor that created the data, DoD may not disseminate or expose the data outside the Government except (1) when needed for emergency repair and overhaul or (2) for limited use by foreign governments for evaluation or information.

Generally, the degree of rights DoD takes in specific technical data is determined (as required by statute) by the source of funding used to develop the data or the item or process to which the data pertain. So, for example, when the item, component, or process has been or will be "developed exclusively with Government funds," DoD can take unlimited rights (but it does not have to do so). If development took place exclusively with private funds, then DoD takes limited rights, unless the contractor is willing to negotiate to give DoD a higher category of rights in the data. And if both the Government and the contractor (or subcontractor) have contributed funds toward developing the item, component, or process ("mixed funding"), DoD is required by statute to negotiate the degree of rights it gets. Most often this requirement leads to a bargain in which DoD takes GPLR for a set period at whose expiration DoD will automatically receive unlimited rights.

There are a number of exceptions to this source-of-funding rule for determining rights. For example, DoD can always take unlimited rights in the following kinds of data, regardless of who funded the development:

- Technical data resulting directly from performance of experimental, developmental, or research work specified as an element of performance under a Government contract or subcontract
- Form, fit, and function data pertaining to items, components, or processes required to be delivered under a Government contract or subcontract
- Manuals or instructional materials for installation, operation, maintenance, or training purposes
- Technical data constituting corrections or changes to Government-furnished data
- Technical data that are "publicly available" or that have been disclosed by the contractor or subcontractor with no restrictions on release.

It is significant that the way DoD defines the phrase "developed exclusively with Government funds" in the regulation is broader than the words themselves would imply. The phrase is defined to mean that "the cost of development was paid for in whole by the Government or that *the development was required for the performance of a Government contract or subcontract.*" [emphasis added] The phrase "required for the performance of a Government contract or subcontract" is further defined to mean that "the development was specified in a Government contract or

subcontract or that the development was accomplished during and was necessary for performance of a Government contract or subcontract."

Offerors and contractors that want to restrict DoD's rights (that is, make them anything less than unlimited) in particular data under a specific contract must give DoD advance notice of any restrictions they wish to assert. This step must be taken prior to delivery of the data. Offerors are required to identify in their proposals any items, components, or processes intended for use in performing the contract that would result in delivery of technical data with other than unlimited rights. This information may be used by DoD in source selection (such as for life-cycle cost analyses), but the statutes prohibit DoD from excluding an offeror solely for refusing to sell or relinquish its legitimate rights in technical data. Contractors must continue this notification process during contract performance. The contractor or subcontractor must submit sufficient information to support any assertion of less than unlimited rights. The contracting officer is supposed to presume the validity of the assertion unless there are reasonable grounds to question that validity. If there are such reasonable grounds, the contracting officer may challenge the assertion and require the offeror or contractor to provide adequate evidence to support it. Continuing conflicts are resolved under the contract disputes process.

The contractor must also mark any technical data it delivers with less than unlimited rights with restrictive markings set forth in the contract. Data received by DoD without these markings will automatically be taken with unlimited rights. However, the contractor may, within 6 months of data delivery, request restrictive markings for delivered data if it can (1) demonstrate that the omission was inadvertent, (2) establish that restrictive markings are authorized, and (3) relieve the Government of liability with respect to the technical data.

Notwithstanding these general rules, DoD may negotiate with a contractor or subcontractor to permit the Government to take more than limited rights in privately funded data. The additional rights may be acquired by negotiating a lump-sum fee, royalty, GPLR, or other arrangement. However, the contracting officer may negotiate greater rights in privately funded data only if there is a need to disclose the data outside the Government for competitive procurement and the anticipated savings from competition are likely to exceed the cost of the data and the additional rights.

Likewise, when a contractor requests the exclusive right to commercialize a technology, DoD may agree to take GPLR rather than unlimited rights. However, these GPLR are for a stated period only. At the lapse of that period, DoD will automatically gain unlimited rights.

For development or production of major systems, the contracting officer is generally prohibited, by statute, from requiring offers that would enable DoD to competitively reprocure identical items or components of the major system, if the item or component was developed exclusively at private expense. An exception can be made to this rule only if the contracting officer determines that

- The original supplier of the item or component will be unable to satisfy program schedule or delivery requirements, or
- Proposals by the original supplier to meet mobilization requirements are insufficient to meet the agency's mobilization needs.

A final provision of the regulation worth noting is the endorsement of deferred delivery and deferred ordering of data. As the regulation states,

> Technical data . . . are expensive to prepare, maintain and update. By delaying the delivery of technical data . . . until needed, storage requirements are reduced and the probability of using obsolete technical data . . . is decreased. Purchase of technical data . . . which may become obsolete because of hardware changes is also minimized.

Accordingly, the regulation contains a Deferred Delivery clause permitting the contracting officer to require delivery of data at any time until 2 years after Government acceptance of all contract items. A Deferred Ordering clause is also provided, for situations in which a firm data requirement is not established. Under this clause, the contracting officer may order any technical data generated as part of the performance of the contract until 3 years after acceptance of all items or after contract termination. When data are ordered under the Deferred Ordering clause, the delivery dates are negotiated and DoD reimburses the contractor for converting the technical data into the prescribed form. The cost of creating the data themselves is not further reimbursed, since the Government has already assumed that cost under the contract.

DoD Instruction 5000.2, Part 9, Section B, Technical Data Management (23 February 1991)

This instruction provides some basic guidance for DoD technical data management. Among other things, it repeats the DFARS injunction that

> Only the minimum data needed to permit cost-effective support of research, development, production, cataloging, provisioning, training, operation, maintenance, and related logistics functions over the life cycle of the item will be acquired.

The instruction also directs that

> Production contracts must include product drawings and associated lists for items that will be reprocured or manufactured in-house. When appropriate, the data package will include information suitable to compete replenishment of subtier spare parts including part level acceptance test procedures.

The term "product drawings and associated lists" is defined elsewhere (see below), but basically it means engineering drawings and other technical data in enough detail to permit others to manufacture the item or component (including any part). This provision thus says, essentially, that whenever DoD intends to establish alternative sources for items or components, it must contract with the original manufacturer for delivery of detailed technical data. But remember that DoD can reprocure an item or component from a source other than the original contractor only when it has unlimited rights, GPLR, or some other license negotiated with the original source.

MIL-T-31000, *General Specification for Technical Data Packages* (15 December 1989)

This document provides greater detail about what is required when technical data are delivered to DoD under a contract.

Product drawings are defined in the specification as

> Engineering drawings that provide the necessary design, engineering, manufacturing and quality support information necessary to permit a competent manufacturer to produce an interchangeable item which duplicates the physical and performance characteristics of the original design without additional design engineering or recourse to the original manufacturer.

Elsewhere, the document states that

> Product drawings and associated lists shall provide the necessary design, engineering, manufacturing, and quality assurance requirements information necessary to enable the procurement or manufacture of an interchangeable item that duplicates the physical and performance characteristics of the original product, without additional design engineering effort or recourse to the original design activity.

Product drawings are to be required in contracts "whenever there is current or future need for the Government to procure or manufacture the equipment, components, or spares and repair parts from either the original equipment manufacturer or an alternate source."

Commercial drawings are defined as drawings "prepared by a commercial design activity, in accordance with that activity's documentation standards and practices, to support the development and manufacture of a product not developed at Government expense." The specification states that

> Commercial drawings and associated lists shall provide engineering and design disclosure information in support of end items that are commercially developed items, off-the-shelf items, *or items not developed at Government expense* [emphasis added]. These drawings and lists are prepared in accordance with the design documentation practices of the contractor or supplier of the item.

Elsewhere the document states that

> Commercial drawings and associated lists are used to obtain existing information regarding commercial off-the-shelf items acquired by the Government *as end items* [emphasis added]. They are not intended to be used to document commercial items used as components in end items developed at Government expense.... Commercial drawings and associated lists should not be acquired as a substitute for product drawings and associated lists when the item is designed at Government expense.

Finally, MIL-T-31000 incorporates several DIDs setting forth format and content instructions for different levels of data. The DID for product drawings and associated lists (DI-DRPR-8100, dated 11 September 1989) states that

> Product drawings and associated lists shall provide the design disclosure information necessary to enable a manufacturer of similar products at the same of [sic] similar state of the art to produce and maintain quality control of item(s) so that the resulting physical and performance characteristics duplicate those of the original design.

The content of product drawings must include, among other things,

- Details of unique processes (i.e., not published or generally available to industry, when essential to design and manufacture)
- Critical manufacturing processes and assembly sequences
- Physical characteristics, including form and finish
- Details of material identification, including heat treatment and protective coatings.

Significantly, the DID closes with the following:

> 10.8 *Limited rights-in-data items.* Product Drawings for items for which the government does not have unlimited rights in data shall specify the form, fit and function requirements of the item and conform to 200.4 of DOD-STD-100.

The comparable DID for commercial drawings (DI-DRPR-81003, dated 11 September 1989) says, with regard to content: "Commercial drawings and associated lists shall provide sufficient information to permit Government maintenance, modification, and engineering analysis of commercially developed items."

As we discuss in Chapter 8, several details and aspects of these policy documents provoke conflict with industry groups and defense contractors.

CHAPTER 3

THE CALS CONCEPT

BACKGROUND

During the last two decades, American industry has experienced severe competitive pressure from companies all over the globe. In response to that pressure, U.S. firms have taken steps to cut costs and speed the development and introduction of new products. One of the critical steps taken has been harnessing the power of the computer through concurrent engineering, CAD, and CAM techniques.

In the past, design engineers worked on their design for a product with little or no input from production or logistics engineers. When they were finished, the product design was then passed to the production engineers, who would make engineering changes necessary to achieve economical, high-rate production. After those manufacturing engineering corrections, the design was often too "frozen" for the logistics engineers to introduce supportability considerations. As a consequence, products had higher operating and support costs and higher total life-cycle costs than would have been the case if logistics engineering had been incorporated at an early stage. And the whole sequential process took a long time.

Concurrent engineering corrects these deficiencies by bringing the design, manufacturing, and logistics functions together at the outset. Each engineering function participates in product design decisions from the very beginning, using sophisticated computer equipment and software for design itself (CAD), computer networks to link and integrate the several engineering elements of the design team and their products, and computer-run equipment and programs that convert the design directly into manufacturing processes (CAM). As a result, companies could manufacture higher quality, lower cost products and introduce them into the market faster.

Much time was also built into the earlier process because, as the developing product passed from one engineering function to another and then on to the marketing and financial functions within the company, the data often had to be translated from one format to another, usually by manually re-keying the data.

Companies began correcting this problem by integrating their internal engineering, logistics, marketing, and financial data bases. This, too, cut the costs and time of bringing a product from development to market. It also provided greater visibility of status and trends, greater corporate coordination and faster reaction to events, and further cost reduction through elimination of redundant actions and through less rework.

During these years of rapid and revolutionary change, DoD fell behind. DoD acquires vast quantities of engineering drawings and other technical information pertaining to the systems and products it buys. The data have been in the form of paper documents or equivalent microfilm images, which can run to thousands of pages for some items. As DoD contractors adopted automated techniques (such as concurrent engineering and CAD and CAM systems), they acquired the capability to design and build major weapon systems completely by computer, without using paper at all. But DoD still required delivery of technical data in paper (or microfilm) form. This requirement meant that contractors had to transcribe their integrated, computer-readable ("digital") data into paper form for DoD review and use. As the complexity of weapon systems increased, the amount of information being generated on paper grew and threatened to overwhelm DoD's paper-based system. Some elements of DoD did automate some of their functions. But since no common exchange standards existed to permit the various automated systems to communicate with each other or with the contractors' systems, "islands of automation" were created without bridges between them.

This situation led to the creation of the CALS program in DoD. The CALS concept envisions eventual computerized delivery and use of contractor-developed technical data. Initially, CALS will serve as an umbrella program to develop and impose data exchange standards on computer hardware and software vendors in order to achieve greater systems interoperability and increase DoD's capability to accept digital data deliveries. It will also build bridges between the various existing automated systems. A further goal of CALS is to provide integrated data bases for weapon systems developed for DoD, with computer access to all information related to those systems by all authorized users of that information. CALS will link, by computer network, all acquisition, design, manufacturing, and support functions that generate or use system-related technical data.

The potential benefits of CALS to DoD can be enormous. The system will permit much faster transfer, review, and revision of data than the current paper system allows. The system will not only greatly increase the efficiency of use of technical data, but will also enhance quality, completeness, currency, and accuracy. Contractors should benefit through reduced costs, increased quality, and faster review of data deliverables.

IMPLEMENTING CALS

CALS has been a joint effort between DoD and industry from the outset. DoD established a high-level DoD CALS Steering Group, while industry organized a corresponding CALS Industry Steering Group. Industry has invested considerable time and money in developing and coordinating CALS issues, standards, and specifications with DoD through the steering groups and subordinate task groups.

But before industry was ready to make a wholehearted investment in CALS, it needed a firm commitment from DoD that CALS was truly going to happen and was not just a passing enthusiasm. That commitment was made in an August 1988 memo from then Deputy Secretary of Defense William H. Taft IV to the Secretaries of the Military Departments and the Director, Defense Logistics Agency. The memo directed all program managers of systems in full-scale development or production to review their programs for possible change of paper data deliverables to digital delivery or access using CALS standards. It further directed that, for all systems entering development after September 1988, solicitations should require schedule and cost proposals by all offerors for integrating contractor technical information systems, Government access to contractor data bases, and delivery of digital technical data. These CALS elements of the offerors' proposals were to be given "significant weight for their cost and quality implications in source selection decisions." DoD components were directed to program for the systems necessary to receive, store, distribute, and use CALS-compliant technical data.

CALS is to be implemented in two carefully managed steps. CALS Phase I, covering the period from inception of the program about 6 years ago through 1992, has focused on developing standards that will govern the electronic exchange of digital technical data between DoD and its contractors. To date, standards have been established for both text and graphics, and a commercial standard has been adopted for querying data bases.

In Phase I, the emphasis has been on improving the transmission of data rather than on the content of the data being delivered. Essentially, the same data formerly delivered in paper form can now be transmitted electronically to DoD by using the standard CALS data formats. But because of current limitations in telecommunications capabilities, the engineering drawings and other technical data are being recorded on tape or optical disk and physically delivered by mail or other means to DoD. Technical data describing a particular product in detail ("product definition data") are still in the same two-dimensional form familiar to readers of paper engineering drawings. So the only real difference between CALS Phase I and the previous system is in the form of the data – computer-readable tape or disk rather than paper or microfilm.

As stated in Chapter 1, this means that issues of data security and control under CALS Phase I are not radically different from before. The contractor still has control over the content and destination of the data being delivered to DoD. Contractors are still able to limit release of data to those data considered explicitly required by contract after appropriate corporate review and approval. Disputes over the quality, quantity, and type of data and over rights in data can be resolved before final delivery and acceptance. Because CALS Phase I has not significantly changed contractors' control over technical data, or the overall security of the data, it has been supported by industry.

PHASE II ISSUES

This is not the case with CALS Phase II. The centerpiece of Phase II is the IWSDB. Under this concept, all technical data relevant to a particular weapon system will be integrated in a data base linking all sets of data and accessible to all authorized users of the data nearly instantaneously upon demand. Even though discrete sets of data may reside in different locations, a user will be able to access at a single computer workstation all of the data for which he is authorized access. In fact, several users may be able to access the same data at the same time.

These changes would permit processes that formerly took place in sequence to be performed simultaneously. The Phase II system would also eliminate the costs of maintaining duplicate data bases and would reduce the inconsistencies that now can develop between data bases as a result of delays in transmitting and receiving updates of changes made to the weapon systems and their technical data. And,

unlike the familiar two-dimensional engineering drawings of the paper system and Phase I, product definition data in the Phase II system would appear as three-dimensional graphics that would permit actual manufacture of the item.

The IWSDB is closely linked to another key Phase II concept, the CITIS contract. Under the CITIS concept, DoD would permit the contractor to deliver data "in place" at the contractor's site rather than to DoD data base locations, as long as DoD is given electronic access to the data. In other words, DoD's physical possession of technical data would be replaced by guaranteed access to the data at the contractor's location.

These Phase II concepts introduce a radically different environment for data security and control. Correspondingly, the issues and conflicts with contractors that might have to deliver their technical data into such a system have mushroomed in number and intensity.

In the past, a requester might require data that had been stored in a half-dozen or more different data bases and would have to apply for access approval ("log in") at each data base to get the needed data. (See Appendix B for discussion of data management and security in the current system.) In CALS Phase II, however, the requester would log in to the network only once, with immediate access to all authorized data within the network. The computer system would instantaneously draw for the user all authorized data relevant to the specific request from the various CITIS data repositories.

Previously there were several checks against unauthorized or improper access to sensitive contractor-developed technical data. Now there would be only one. The potential for error and for consequent serious competitive damage to a contractor is increased; sensitive technical data that a contractor must deliver to the Government become much more vulnerable to being exposed to unauthorized users.

And even data not required to be delivered to DoD become more vulnerable. That is because the concept of an integrated data base at the contractor's site involves DoD (and other authorized users) access to a portion of the contractor's internal corporate technical data base. Although a contractor could try to establish controls to put the rest of its internal data base – the nondeliverable, corporate sensitive data – "off limits" to external requesters (both DoD and other contractors), the risk of exposure to people already legitimately inside the CALS network remains great.

Whereas security measures for preventing unauthorized entry into the network itself can be very robust, internal security measures within the network must allow quick access for routine authorized internal use. That is the whole point of CALS – easy, quick access to a significant portion of the contractor's corporate technical data base. The internal security measures will thus necessarily be weaker than measures focused on defending against external penetration, and it becomes easier for a competitor with access to the system to penetrate a contractor's sensitive data repository.

Even if a competitor did not specifically attempt to gain unauthorized access to a contractor's sensitive data, it might take advantage of the integrated data base capabilities to "browse" through various authorized parts of the contractor's data and accumulate enough nonsensitive information to derive sensitive information from it. This is known as the "aggregation" problem. It is familiar to all who work with classified information. Individual bits of information may not by themselves be sensitive, but when they are gathered together and analyzed, the whole may reveal something greater, more sensitive than the parts.

Another major Phase II question involves who can change data in the system. Authorized DoD personnel will have access to data in the contractor's repository. There is need then for a management system that will identify and distinguish between working, released, revised, and accepted versions of the same data in the same data base. Otherwise, there will be terrible confusion as to the status of the data, the controlling agent, and the owner (or authorized user). Specific controls may have to be placed on all contractor data, rather than just on the data to be released to DoD, in order to protect the integrity of non-DoD data to which DoD has access. An example would be a contractor's internal financial data supporting the financial data submitted to DoD but in themselves not deliverable. Any errors in identifying the status of data in the contractor's data base could result in harmful loss of sensitive data.

Another concern of contractors regarding Phase II is the possibility that DoD personnel may be able to make "ad hoc" queries of any data to which they have authorized access. This capability will allow them to compare normally unrelated data and draw conclusions. Contractors are concerned that such "unsupervised" queries could lead to inaccurate conclusions through mixing of incompatible data ("apples and oranges"), or to aggregation of data into sensitive information that the

contractor can rightfully withhold from DoD. There is the risk that DoD might also "look over the contractor's shoulder" during contract performance, resulting in unnecessary explanation, justification, cost, and delay.

The sum total of these contractor concerns is fear that the CALS concept will produce *de facto delivery* of contractor-sensitive data, regardless of whether or not the data are legally required under the contractor's development or production contract. These concerns add to, and intensify, already existing conflicts over what data should be required to be delivered and what uses DoD should be able to make of the data.

Any CALS-type integrated data base system will – by its very nature – offer greatly increased likelihood of exposure of contractor-developed data to other system users, compared to the current system of storing paper documents in Government repositories where physical access can be tightly controlled. Imposing the kind of security controls used in a classified national security network would stifle the accessibility and rapid exchange of data that are the hallmark of CALS. As long as contractors have to deliver data that they regard as vital to their own economic health into a computer-based system that permits widespread access by potential competitors, they will regard that system as inherently threatening to their vital interests. Thus, unless the longstanding conflicts over DoD technical data policies requiring delivery of sensitive contractor data are satisfactorily addressed, contractors will not fully support a CALS-type integrated, computer-driven data system. DoD technical data policy and CALS data security issues must both be satisfactorily addressed before CALS implementation can proceed with a high degree of industry support and cooperation.

CHAPTER 4

TECHNICAL DATA AND THE MARKETPLACE

THE VALUE OF TECHNICAL DATA

Companies try to distinguish themselves from others in their lines of business in order to attract buyers. Effective marketing, competitive pricing, and good customer relationships are key elements of this effort. But in an increasingly competitive world marketplace, probably the most important factor of all is the quality of the product or service being sold. Technical data constitute the record of all the characteristics of a company's products and processes and the way its products are manufactured. Technical data thus document the quality of a company's products and are at the center of a company's efforts to differentiate its products from those of its competitors. Therefore, the information contained in technical data is critical to a company's success (or failure).

Technical data can take many forms for many different uses, and not all those forms reveal vital company information. For instance, data such as technical manuals for installing or using the product or for minor repair and maintenance do not, by themselves, contain enough detail about the products, processes, or underlying technology to enable someone else to make the specific product – or other products using the same technology.

Companies usually regard as very "sensitive" their technical data that give a detailed, complete description of the product – often called detailed design data or product definition data – and data that record the techniques and processes necessary for production – often called manufacturing process data or, simply, manufacturing data. That is because these functional types of technical data in the hands of a competitor could enable, or significantly help, that competitor to make the company's product at the same quality or to make other competing products using the company's technology. These types of data are understandably regarded as much more sensitive than, for instance, manuals for installation, normal use, minor repair and routine maintenance, and personnel training.

PRODUCT DEPENDENCIES

One or Few Products

Besides the degree of vital detail revealed by the functional types of data, another consideration determining how critical particular data are to a company is the degree to which that company depends on sales of the related product or technology. A company with only one product or unique technique or process is totally dependent for survival on the market success of that product or process. Such companies will naturally be extremely protective of the types of data that would permit anyone else to produce the product or otherwise make inroads upon some or all of the company's sole source of revenue. They will generally try to prevent exposure of the data to *anyone* outside the company, for fear that the data might somehow get into the hands of a potential competitor.

Commercial Applications

A second kind of product "dependency" occurs when the data, in whole or in part, can be successfully applied in a second lucrative market in addition to the one for which the data were originally created. For example, product technical data that a company develops originally for sale to DoD for a military item become much more valuable to the company when they also have an application for a commercial market, since they become the vehicle for a much greater stream of income than if restricted to the Defense market only. Furthermore, when the commercial market represents a potentially larger source of income than the military one, the company will be extremely reluctant to jeopardize the greater market by risking sensitive data in the lesser one.

In building a major DoD weapon system, usually a single prime contractor will be charged with managing the overall job. That prime contractor will have to coordinate the efforts of thousands of suppliers (subcontractors) that will contribute their parts, processes, and work and services to the finished product. Most of the material and components (represented by cost) of major weapon systems come not from the prime contractor but from subcontractors and suppliers. The range of subcontractor contribution to a major weapon system has been held to be from 50 percent to 85 percent, in one study [4]. In an LMI study of manufacturing

technology process costs, the average cost of purchased parts (subcontractor contribution) for major weapon systems was found to be 60 percent [5].

Accordingly, the bulk of technical data for major weapon systems originates with subcontractors. Some prime contractor representatives admit that their companies have relatively little proprietary, sensitive technical data that they must protect. In some cases, the subcontractors contribute a standard commercial part or component that is indistinguishable, or virtually so, from the item that they sell to commercial buyers. DoD (or, more accurately, the prime contractor) is merely another customer. And, although the whole program may be worth billions of dollars, the subcontractor's participation may be only a single component, and units of defense major systems are usually smaller in number than comparable commercial runs.

In other cases, an item may be custom-designed for the weapon system, yet its internal composition can be almost entirely of commercial parts. Heat exchangers, for example, have to be designed to fit the particular cabin space of an aircraft, often with many changes as the cabin design undergoes revision. But the materials and construction technology (the welding and other means of fastening) used, which comprise the core of the art of manufacturing and repairing these components, are used both in military and civilian aircraft. The technical data recording these materials and processes are thus extremely sensitive to a company in the business of selling heat exchangers. Similarly, while auxiliary power units generally have a different end-item number for commercial and military products, 80 percent of the internal composition of the military item usually consists of commercial parts. These parts are normally built on the same production line, whether they are for military or commercial use.

High-Technology Products

A third kind of dependency occurs in the sale of high-technology products and processes. That is because these products require heavy investments in R&D while experiencing very short product lives because of rapid obsolescence due to technology advances. The only way for such products to be economically viable is for the company to control a very high market share for the short life of the product. Exposing the underlying technical data to competitors would threaten that market control.

Companies regularly invest in research to develop new technologies and products that can be sold in their markets. The companies then use the revenues from product sales to pay back the cost of the product and technology development and to help finance new investment in development of future products. Some areas of business, such as high-technology products and processes, tend to be more risky research investments than other areas are. That is because research in them generally yields fewer products that are ultimately successful in their marketplace than does research in other areas. This means that those few successful products must produce much more income than other products in order to pay for the greater amount of research necessary. One strategy to ensure such substantial returns is to protect a monopoly position in the product or technology so that a premium price (often called a monopoly "rent") can be charged. Of course, this premium price can be successfully charged only when buyers believe that no comparable cheaper product is available.

The premium price is viewed by some as an artificial windfall to the monopolist and by others as a charge absolutely necessary for recouping research costs and funding investment in further research. It is thus very much a matter of judgment as to whether that price is ultimately "fair" or "reasonable." In making such a judgment, one might consider such factors as

- Is the premium price necessary to recover actual research costs, and were those research costs themselves "reasonable"?
- Is the premium used to finance future necessary product research?
- Is the premium a necessary reward for the risks assumed and a necessary inducement to make further investments in high-risk product areas? Some product markets (such as drugs and high-technology product areas) involve very high likelihood of failure. Companies considering investments in product development in those areas will not make the investment when the risk is very high, the investment costs are high, and the potential return on the investment is comparatively low. Rather, they will put their money into more rational alternative investments. And society ends up the poorer for this, because (for instance) the life-saving or life-enhancing drugs and other products will not be created.

In recent years the cost of R&D has soared. At the same time, the pace of technological change has accelerated; new technologies and products are outdated more quickly. Thus the time available for recovering the research investment costs

has been cut sharply. So, for example, 17 years of patent protection may be meaningless, because the actual life expectancy of the product is only a few years.

To cope with these changes, companies have adopted a number of strategies. For one thing, they are working harder at better targeting of R&D projects, so that they have a higher success rate and quicker payoff from their research investments [6]. They are also trying to protect their technologies and trade secrets (recorded as technical data) even more ferociously than before, in order to extend the effective life of the products and processes. And they are teaming together in joint ventures that share R&D costs, thereby reducing the amount each company has to recover and the amount of its risk exposure (but also reducing the amount of revenue).

USE AND PROTECTION OF DATA

Together with the type of data and the degree of economic dependency, another factor to consider is the use of the data outside the company itself. Release of technical data damages a company only if the data end up in the hands of an entity that exploits them to the company's economic detriment. Therefore, the way particular data are used and protected can determine their ultimate value. The degree of exposure the data are given, to whom they are given, and under what kinds of controls – all these matters directly affect the economic utility of the data. So, for example, a company may allow a prospective buyer's engineer to review certain product engineering drawings for purposes of competitive evaluation against other proposed products, provided the buyer is not a potential competitor, the examination is performed at the company's plant in the presence of a company employee, and the documents are immediately returned to the vault. Or a company may license another company to use its technical data, usually with very tight restrictions prohibiting (and severe legal penalties for) licensee release or exposure of the data to third parties. On the other hand, a contrast to these carefully controlled releases of data would be a buyer's widespread distribution of a supplier's sensitive company data to that supplier's potential competitors, or a situation in which the company creating data publishes or exposes the information either deliberately or by error, in a way that makes it widely available. For further discussion of licensing and protecting data, see Appendix C.

TECHNICAL DATA AND COMMERCIAL PRACTICE

In commercial sales of high-technology products, sellers generally include sufficient form, fit, and function information to allow the buyer to operate, store, and transport the product. Form, fit, and function data are also provided to support maintenance of the product to the extent that the buyer is expected to perform that maintenance. Design or manufacturing process information of use mainly for modification or manufacture of the product is generally not provided to the buyer.

If the buyer has a specific need for design or manufacturing process data, the buyer generally negotiates with the seller for the data on a case-by-case basis. If the seller agrees to release the information, the seller will generally require nondisclosure protection (often in the form of a license) and will usually provide technical assistance to the buyer to ensure that the technology is used properly (e.g., for maintaining quality, structural integrity, etc.).

SUMMARY

Companies in both the defense and commercial marketplaces regard certain kinds of technical data as extremely vital to their economic health and even survival. Technical data are considered vital if they capture enough detail of a product, process, or underlying technology to enable a competitor to take business away from the company. (Usually, these are detailed design and manufacturing data.) Data relating to products and processes on which the company depends heavily are also vital. A company may be dependent because it has only one or a few products or special processes to sell; because it is in a high-technology business that requires control of a high market share to recoup R&D investment; or because the product, process, or underlying technology has applications in more than one market. Companies will zealously protect their vital data from any possible exposure to competitors or potential competitors.

Most of the value of today's weapon systems comes from subcontractors. Many of these subcontractors are extremely dependent on the product, process, or technology they contribute to the system. In addition, major weapon systems often incorporate state-of-the-art technologies vulnerable to rapid obsolescence. And much of the technical composition of a system (especially the underlying technologies and processes) will typically have a commercial application as well as a military one. For a large segment of the contractor and subcontractor population, all of these factors –

dependence, high-technology competitive market, and commercial applications – are operating. This is to say, then, that a very large part of the typical value of a weapon system is represented by technical data that are extremely sensitive to the originating company.

Furthermore, whenever a company sells items both to a commercial market and to DoD (as a separate item, as a military item incorporating commercial parts or components, or as a military item incorporating technology with potential commercial applications), that company will have reference to the foregoing facts of commercial life. The defense marketplace will be compared to the commercial marketplace for attractiveness of business and safety of vital company properties, such as critical technical data.

In such a comparison, as we shall see, DoD's contractors and subcontractors are finding the defense marketplace unfavorable. This perception has significant adverse consequences for DoD's ability to perform its national security missions.

CHAPTER 5

CONFLICT OF INTERESTS

The Department of Defense uses various levels of detail of technical data pertaining to weapon systems, depending on the use that is to be made of the technical data. Generally, the data are used for recognized, noncontroversial operational needs, such as installing the item or component; routine maintenance and repair; or training DoD personnel to use, repair, and maintain the equipment. Normally, these operational uses require no more detail than is contained in form, fit, and function data. Contractors and subcontractors have no objection to such uses or to DoD's acquiring this level of data from them. In the commercial marketplace, sellers usually give buyers technical data with similar levels of detail.

But DoD also acquires the detailed design and manufacturing technical data of its contractors and subcontractors. The primary reason DoD acquires such data is to be able to establish alternative sources. This practice may take the form of creating a second source for production of an entire weapon system or major component (such as an engine), or it may be to establish alternative suppliers for smaller components and spare parts.

Two principal reasons are cited for establishing alternative sources. One is to influence price. By establishing other sources, DoD hopes to introduce competition to get prices down and keep them down during the life of the weapon system. Historically, this has been the primary reason for DoD's policy of establishing alternative sources, as we have noted in discussing the evolution of DoD's technical data policies (see Chapter 2 and Appendix A). This is not an operational need but an economic one. Thus, it can be contrasted with the clear operational needs cited above.

As noted in Chapter 1, in recent years, DoD has cited an additional reason for establishing multiple sources for systems, components, and parts. That reason is the need for many potential sources of supply to respond to sudden demands for increased production in national emergencies. These sudden emergency production increases are known as "surge" requirements (for short-term national security events such as

the Persian Gulf War) and "mobilization" requirements (for events on the scale of a world war).

Besides needing contractors' design and manufacturing data to establish alternative sources (to control prices and be able to meet surge and mobilization requirements), DoD also cites two other uses for this kind of data. It declares that it needs the data in order to guarantee a source of supply if the original contractor can no longer perform or refuses to continue to perform the contract. And it cites the need to perform emergency overhaul and repair of systems, such as ships, which may require using the manufacturer's design or manufacturing data in remote locations. This (often contracted-out) work can require detailed design data (especially when repair involves virtually remanufacturing elements of the system) or other information that the original contractor may regard as proprietary information important for its business. For some contractors, aspects of major repair are held as a trade secret. For example, in repairing aircraft clutch elements, there may be many ways of taking the package apart and putting it back together. But only one way works. Companies may regard knowledge of that "one way" as a trade secret, because it gives them an important advantage in the repair and overhaul side of the business, both commercial and defense. These contractors are likely to protest having to surrender such technical data to DoD.

As we have noted previously, proprietary design and manufacturing data are precisely the data that contractors and subcontractors regard as their most vital and sensitive technical data. And the use to which DoD puts the data – handing them over to other suppliers that may become competitors – is precisely the exposure that most threatens the original company's vital interests.

Thus, DoD and private companies are in direct conflict over DoD's need for and use of the companies' design and manufacturing data. Although some contractors and subcontractors may profess objections to DoD's "confiscation" of *any* proprietary data, the real interest on the contractors' side is in protecting vital, proprietary design and manufacturing data.

But what is proprietary? In discussing the evolution of DoD data rights policy (see Appendix A), we note that the definition of "proprietary" has been controversial, murky, and changing. Today, industry representatives generally concede that DoD has a right to unrestricted use of all levels of data related to products for which DoD

has provided all the development funding. On the other hand, most would insist that, at a minimum, any data related to an item that the contractor developed completely at its own expense are proprietary to that company.

What happens when the original source of funds for development of a particular item is unclear, or not known? What happens when both the Government and the contractor have contributed some funds to development and the funds have been so mingled that it is virtually impossible to segregate those aspects of the final item that derive from Government funds from those that derive from private funds? Or a privately developed element may be incorporated into a larger item or component in a way that makes the element indistinguishable or inseparable from the larger item, which may be Government-developed. Is the proprietary nature of the element lost in the larger "sea" of the nonproprietary item?

It is sometimes argued that some defense industry companies have done nothing but Government work from their very birth and that therefore all of their technical data have their origins at some point in Federal funding. But the counter-argument can be made that even companies totally dedicated to DoD work from their inception nevertheless raise capital through sale of stocks and bonds, through loans, and from other private sources completely independent of the Government. These sources of capital can be used to fund independent research and development (IR&D) projects with the goal of eventual sale to the Government. Such independently funded work would be regarded by the company as proprietary (and is acknowledged as such in the DFARS).

The fact is that the precise original source of funds for the development of an item, component, part, process, or technology often cannot be determined. This ambiguity exacerbates the conflict between industry and Government over rights in technical data, especially when the needs of the parties are directly contradictory.

In addition to objecting to the delivery of their proprietary technical data to potential competitors, contractors regard the establishment of alternative suppliers, by whatever means, as contrary to their vital interests. That is because, obviously, the alternative sources directly take away some of the defense business under the particular production contract that otherwise would have gone to the original contractor. This concern has been exacerbated in recent years by the practice of

underfunding the development work that takes place prior to production and by the decline, because of budget constraints, in the numbers of items being produced.

In major weapon system acquisitions, there has long been intense pressure on industry to put up a significant portion of the system's development costs. The real costs of development for a weapon system are much higher than the funds appropriated by Congress, and the defense industry has been subsidizing those extra costs. In part this situation derives from an unwillingness on the part of DoD or Congress to pay for the true, higher costs of development. In part it derives from the intense competition between prime contractors for award of the production contract. This practice has been reflected in the use of fixed-price contracts for DoD developmental work. The sums paid to contractors under such contracts have not covered the actual costs of the work performed. In the long run, this development cost sharing can be economically endured by industry only if the costs borne by the contractor are recouped in the production phase of the program. No one stays in business by spending money not recouped in sales.

In hearings conducted by the Senate Armed Services Committee in 1988, David Packard, head of Hewlett-Packard Co. and chairman of the 1986 Presidential commission on defense management and procurement popularly known as the Packard Commission, testified that the defense industry had picked up $10 billion of this unreimbursed investment. But because DoD usually insists on dual sourcing the production, contractors generally cannot recoup the development investment. Packard predicted that continuing the practice of forcing contractors to bet their companies on winning the production contract and then breaking the production into two uneconomical packages will eventually result in the bankruptcy of many of these firms or else in their nationalization. Packard said that the Defense Department was "way off base" in requiring commercial suppliers to furnish data rights to second sources [7]. This situation is also highlighted in a recent report of Congress' Office of Technology Assessment [8].

To recapitulate, defense contractors and subcontractors object to DoD's practice of alternative sourcing for systems, components, and parts because this practice cuts into their revenue. Their objection is enhanced when DoD development contracting practice forces development contractors to invest significant funds that cannot be recouped because the production levels for the development contractor are too low as a result of second sourcing, lower budgets, or both. Defense contractors also strongly

object to DoD's practice of giving their proprietary design and manufacturing data to potential competitors, whether for alternative sourcing or to cover unusual circumstances. When all these factors are combined, there are grounds for a dramatic conflict between DoD and its suppliers.

Defense Department policies and contracting rules directly affecting the acquisition of contractors' proprietary design and manufacturing data are set forth in the DFARS and in other documents described in Chapter 2. Contractors protest that these rules force them to surrender their most vital and sensitive proprietary data under a number of circumstances. They specifically cite the DFARS definition of "developed exclusively with Government funds," discussed in Chapter 2. In the view of many industry representatives and legal experts, DoD has defined this phrase so broadly that it potentially embraces *any* data that a contractor might incorporate into a weapon system under a contract. Under this definition, any contractor developing an item or process with its own funds before or during contract performance (not charging the development cost to the Government) and incorporating that item or process into a weapon system risks having DoD acquire unlimited rights in the data.

Another troublesome DFARS provision gives DoD unlimited rights in all technical data resulting directly from the performance of experimental, developmental, or research work specified as an element of performance under a Government contract or subcontract. Again, the concern of contractors is that they may incorporate sensitive proprietary data in their work under the contract and that the data will be swept in to DoD with unlimited rights and later exposed to outside competitors. When the R&D work is intended to increase basic knowledge in a particular technological area (such as might be funded by the Defense Advanced Research Projects Agency, for example), industry does not generally object to granting DoD unlimited rights in the resulting data. After all, that is the whole purpose of such an R&D effort – to develop knowledge and disseminate it freely. And to do that DoD must have unlimited rights in the data, by definition. Obviously, however, much R&D effort is clearly preparatory to the production of an item for DoD. It is in this category of development work that contractors protest the potential loss, as a result of this DFARS provision, of proprietary information that they incorporate in the effort.

In mixed funding situations, the regulations provide for DoD to take GPLR, which supposedly allow the originating contractor the exclusive right to commercialize the data. But DoD may expose the data to other potential sources as part of the process of seeking additional suppliers. While potential bidders for this later manufacturing must certify that they will not use the data for their own commercial purposes, contractors regard this certification as virtually meaningless. The fact is, once the knowledge captured in design and manufacturing data is revealed to another qualified manufacturer, the secret is out and cannot be recovered. And it is almost impossible for the original source to prove that the second source expropriated the data for its own commercial advantage.

With regard to DoD data delivery requirements, contractors point, for example, to the MIL-T-31000 requirement that contractors deliver "product drawings and associated lists," defined to include all data necessary to enable another source to manufacture the item or perform the process, as we noted in Chapter 2. The effect of this requirement is that contractors must deliver to DoD their proprietary design and manufacturing data, regardless of what uses DoD may make of the data by operation of the rules and contract. Qualifications to this requirement allowing contractors to deliver only form, fit, and function detail when the data are proprietary are ambiguous.

In addition to such policies, which potentially enable DoD to demand contractors' sensitive proprietary data and to use the data in ways threatening contractors' vital interests, contractors allege that DoD contracting practices are extremely aggressive and "confiscatory." Once again, the practices most strongly protested are those driven by DoD's perceived need to have contractors' detailed design data and manufacturing data in order to establish competitive sources. The recently decided case of *Dowty Decoto* perhaps best illustrates contractor concerns in this area.

In the early 1970s, Dowty Decoto, Inc., designed and patented a reusable holdback bar for the landing gear of carrier aircraft, such as F-14s, F/A-18s, and T-45s. The bar was a fitting to release the aircraft when the aircraft was catapulted from the deck. Decoto originally approached the Navy with the design for the bar, and the Navy referred Decoto to Grumman, a Navy prime contractor. Decoto signed a subcontract with Grumman to provide these bars for Navy aircraft, on the express condition that the technical data not be revealed to any third party. The subcontract

stated that the technical data to be delivered would be "a Decoto proprietary item on Decoto format with 'Limited Data Rights'." Decoto never quoted a figure or asked for funds for design effort or production tooling. After testing several preproduction units, Grumman asked Decoto to redesign the product to triple its life. Decoto successfully did so and submitted a change proposal for the additional work. Eventually, Grumman issued a change providing about half the funding Decoto requested. This change money came from the Navy.

In 1983, the Navy challenged the restrictive legends on Decoto's technical data. The Navy wanted to remove the proprietary legends and use the technical data for competitive reprocurement. Decoto responded by saying that the bar had been developed "strictly by private funds." The Navy initially dropped its challenge but then renewed it in 1986. After unsuccessful negotiations, the contracting officer informed Decoto that the Navy was going to remove the proprietary legends and farm out Decoto's engineering drawings to get competition for the component. Decoto sued in Federal district court to get an injunction against the Navy's action.

The district court found the Navy's action arbitrary and enjoined the Navy from removing the legends on Decoto's property. The court held that the Navy was bound by the terms of Decoto's subcontract with Grumman, and that clearly Decoto had "developed" the item entirely at private expense before it ever received Government money to "improve" the item to a degree. The change order and funding occurred after the component had already proved workable (and was therefore considered "developed") and had been used successfully without failure in 42 F-14s. On appeal, the Ninth Circuit Court of Appeals also found the Navy's behavior egregious and sustained the district court's permanent injunction [9, 10].[1]

This case is not isolated, nor is the drive to introduce competition limited to the Navy. A recent commander of the Army Materiel Command told Army program executive officers and program managers that they must push for competition in all Army programs, including challenging contractor proprietary data claims. The general told the officers

> If we can afford it, we'll want tech data packages suitable for competition for all components and spares. We'll . . . want to reduce or eliminate proprietary data rights. . . . In addition, all future systems will be

[1] Dowty Decoto, Inc., v. Department of the Navy, 883 F.2d 744 (C.A., 9th Cir. 1989).

> evaluated for possible dual-sourcing so that we can reap the benefits of competition throughout the production of an item.

Prime contractors will "be required to have at least two sources qualified for most parts" [11]. These statements are perfectly consistent with DoD policy on competition and are not unauthorized actions. In recent years, contractors and subcontractors alike cite tremendous pressure from the Military Services for prime contractors to demand delivery of unlimited rights in data of all subcontractors, regardless of regulation or custom.

To recapitulate, the fault line of conflict between DoD and its suppliers over technical data lies in DoD's demand for delivery of contractors' and (through the primes) subcontractors' proprietary design and manufacturing data and in the use of the data, especially to develop alternative sources. This DoD policy is implemented in regulations and other policy documents and in aggressive contracting practices that firms believe unfairly confiscate their most vital and sensitive data.

On the other hand, DoD strongly believes it needs such data to establish competitive alternative sources of supply to keep costs as low as possible and to provide for surge emergency requirements. DoD is under great congressional and public pressure to do so. DoD also needs this level of data to start up other sources when the original supplier can no longer perform the contract for supply of the item or refuses to perform. And it needs the data for the relatively rare case of major overhaul, especially in emergencies.

CHAPTER 6

DEFENSE INDUSTRIAL BASE ATTRITION

Absent a national emergency, nobody forces anyone to contract with DoD in weapon system programs. Some would say further that contractors are not forced to surrender their sensitive data and that they do so because they want DoD's business; if they do not want that business, they are free to find work elsewhere.

This would be a persuasive argument if there were no adverse consequences to DoD stemming from its technical data policies and practices. If there is such a vast pool of contractors and subcontractors that all work DoD may want done can be done by several companies willing to do the work even given DoD's policies and practices, then clearly DoD has no concerns. If, on the other hand, DoD's policies and practices with regard to technical data are causing companies to withhold leading-edge technologies from DoD weapon system programs or to refuse to participate in DoD programs, then there is a very serious cause for concern. If the latter situation is the case, clearly U.S. weapon systems are inferior to what they could have been, and their prices may be higher because of diminished competition. But which case is the reality?

We believe that the latter is. In the name of competition, DoD has adopted policies and practices (varying in degree among the Services) that appear to be driving critical firms out of the defense business, thereby reducing the overall quality and degree of competition – exactly the opposite of the effect desired.[1] What is the evidence of this? In the present chapter, we review three types of evidence leading us to this conclusion. Beginning with the weakest form of evidence – anecdotal reports and allegations – we will proceed to discuss briefly the findings of other

[1]It is not clear from available data whether there has been an actual decline in numbers of firms participating in the defense industrial base over time. Such a statistic may be irrelevant, anyway. The question is not so much whether the absolute number is now smaller than before, but rather what is the relative quality of the firms participating? Let us assume that there were 10,000 firms participating in the industrial base in 1980 and 10,000 today. Even though the number has not changed, if between 1980 and 1992 titanium casting suppliers – critical to DoD – have been replaced by ketchup suppliers, there has been a serious deterioration in the industrial base. Or, high-quality, world-class suppliers may have been replaced by lower quality suppliers.

investigators and conclude with a review of several DoD and industry surveys of defense contractors and subcontractors. One very recent survey, performed at LMI's request, yielded significant results that, though not conclusive, corroborate much of what we have discussed in the preceding pages. We will therefore highlight that survey first.

PROPRIETARY INDUSTRIES ASSOCIATION MEMBER SURVEY (1991)

In the summer of 1991, the Proprietary Industries Association, whose approximately 90 member companies are primarily defense subcontractors, conducted a detailed member survey on the subject of technical data policies and practices. That survey is shown as Appendix D. As of the writing of this report, 12 members had responded. Although these 12 certainly do not constitute a large sample, their responses did corroborate some of the results of the other studies and surveys.

Ten of these companies are in the aerospace business. About half characterize themselves as large companies; the other half are small. For the six firms providing sales revenue information, the median annual sales figure was $42.5 million, in a range from $10 million to $1.4 billion. Three-quarters of the companies said that *some* of their revenue is from DoD contracts/subcontracts; the others said that *most* of their revenue is from DoD business.

With regard to the technology costs of DoD data rights policies, 75 percent of the respondents indicated that they had withheld their best or latest technology from a DoD procurement because of data rights concerns. Most of the respondents that had withheld their best technology from a DoD procurement said that they did so "frequently" or "always" over the preceding 5 years. And 75 percent said that they expected to withhold such technology in future DoD procurements because of data concerns. Also, three-quarters of the respondents said that they make privately funded investments in DoD-unique product improvements or development. Of those respondents, 89 percent said they planned to reduce such investments in the future because of data concerns.

With regard to nonparticipation in DoD procurements, 83 percent of the respondents said that they had refused to participate in a DoD procurement because of data rights requirements or had taken exception to data rights requirements in a DoD solicitation. Seventy-five percent of the respondents said that they expected to

refuse participation in at least some future DoD procurements because of data concerns, while 33 percent said they planned to drop out of DoD business entirely. Data concerns were a moderate-to-strong influence on that decision, as compared to other factors such as the shrinking DoD market.

Although not directly related to the issue of attrition, it is interesting to note that the survey found that a clear majority opposed the use of proprietary detailed design data and manufacturing data *for any DoD purpose.* Opposition was particularly strong to the use of such data for dual sourcing, competitive reprocurement, and internal (Government) manufacturing. Interestingly, the survey found significant (though not majority) opposition to the use of form, fit, and function data, especially for dual sourcing, competitive reprocurement, and internal manufacturing. Thus, these contractors were most strongly opposed to the practice of alternative sourcing and to the taking of their design and manufacturing data for any purpose.

What data did these companies consider to be proprietary? With regard to products developed entirely with private funding *prior* to a Government contract, all believed that if the contractor then privately funded a modification to meet DoD contract requirements, all the product data were proprietary. Where the privately developed product is later modified with Government funds, the results were mixed. A plurality among the respondents said that whether the modification was minor or major, if the privately funded elements of the end product could be segregated from the DoD-funded elements, then the privately funded elements were proprietary. If segregation was impossible, then all the data should be considered proprietary. With regard to a product developed *during* the course of a Government contract or subcontract, the results were similar. Where privately funded products are incorporated in the contract end item, the clear trend was to claim proprietary rights to *all* data if the privately funded elements could not be segregated, and proprietary rights to only the privately funded data when they could be segregated. When the company funded part of the end product development and the Government funded the rest (mixed funding) during the course of a DoD development contract, a plurality of the respondents would apply the same segregability rules.

INDUSTRY INTERVIEWS AND COMMENTS

One major category of evidence is anecdotal. In meetings with officials representing several major defense corporations and industry associations (including the Aerospace Industries Association, Council of Defense and Space Industry Association, Electronic Industries Association, National Security Industrial Association, National Tooling and Machining Association, and Proprietary Industries Association), corporate leaders consistently alleged that there were serious problems concerning data rights issues and that these problems are adversely affecting DoD's mission performance.

Without commenting on the accuracy of these representations, we provide a sampling of representative industry expressions.

The Navy's Seawolf program has frequently been cited as a case of excessive zeal for rights in data causing a massive revolt of suppliers that simply refused to participate. The marine machine industry was a significant part of that boycott. "Certain U.S. firms that are internationally recognized leaders in marine technology are not participating in the Seawolf program as a result of the data rights issue," according to Jack Janetatos, director of the Marine Machinery Association, whose members make components such as valves, solenoids, and compressor pumps. "This leads us to believe that they are not producing the most capable boat possible." According to Janetatos, these components are almost all designed completely at private expense, yet the Navy and the prime contractor were insisting on unlimited rights in the technical data and submission of full detailed design and manufacturing drawings. Another industry official familiar with the Seawolf program is quoted as saying that in the long term, if the Navy continues to adhere to its attitude about contractors' technical data, the Navy "will not get the creative base of America" participating in future programs [12]. David Bolca, project manager for the submarine technology program at Bell Labs, stated: "We've got data rights problems in spades. We can tell the Navy to stuff it when we don't like their attitude on data rights. And we have. But smaller companies may not have that luxury" [13].

After his favorable court decision noted in Chapter 5, Dowty Decoto President Bill Wheeler said

> "I think our whole technology base will be stronger if companies can protect their particular area of expertise. I would hope that [the decision] would have some bearing" on whether DoD, particularly the Navy, stops

> forcing companies to give up data rights. "It is an area of concern to a lot of companies. I know a lot of companies that would not bid on the V-22 for instance, because if you got a contract there you had to agree to give up the data rights, and there are a lot of people who just wouldn't bid." [10]

Another industry executive, speaking to an *Aerospace Daily* reporter on condition that he not be identified, said: "I think the Navy's going to have to go back and rethink its position on second sourcing." Another said

> One of the biggest complaints in second sourcing throughout the industry has been that you spend a lot of time and energy and money developing something for the government and you're not really allowed to recoup your investment because they second source and the guy who didn't spend all that money comes in and underbids you. [10]

Thomas Marotta, chairman of Marotta Scientific Controls, maker of valves for Navy ships, NASA satellites, and the space shuttle, said:

> There is great pressure to give up your rights to data. If we refuse, we are disqualified from bidding – even for equipment we've developed ourselves. Our Navy will continue to lose its small business suppliers if these onerous requirements continue. [13]

Although the Navy has probably been the most aggressive of the Services in this area, and thus is most frequently cited by industry, this orientation is widespread throughout DoD. We have already quoted the statements of the former commander of the Army Materiel Command. So, for example, when the Army developed the T-800 engine for its LH helicopter, it demanded delivery of all data with unlimited rights so that it could establish a second source. And in the later program for the main LH helicopter itself, the Army included similar requirements to be flowed down to subcontractors, until those requirements were challenged by the Proprietary Industries Association [3, 14].

OTHER INVESTIGATIONS

It is often impossible to separate allegation, rhetoric, and positioning from fact in anecdotal evidence such as that given above. Have other investigators found similar results? Yes. Some examples follow.

RAND Study of IR&D

A recent RAND Corporation project investigated the effects of DoD support of corporate IR&D, which can be reimbursed by DoD as an overhead cost under DoD

cost-reimbursement contracts. The study was conducted for the Office of the Under Secretary of Defense for Acquisition.

The DFARS rules for rights in technical data specifically state that technical data developed under corporate IR&D projects, even though they may eventually receive some reimbursement from DoD, are considered data developed exclusively at private expense and that DoD will receive only limited rights in such data if they are later offered under a DoD contract. But the RAND group found that in recent years the Military Services, and the Army most aggressively, were demanding greater rights in IR&D-developed data. The authors stated

> We cannot comment on the legality of the proposed policy, but we can comment on its probable effects. From our case studies and discussions with corporate IR&D managers, we predict that eliminating contractors' proprietary rights to data will reduce the amount and quality of work performed under IR&D.
>
> If contractors are denied the opportunity to profit from the results, IR&D will be less attractive and they will do less of it. Exceptionally promising projects (and the scientists most likely to produce important discoveries) will be segregated from the IR&D cost-reimbursement pool and funded entirely from corporate sources. As a result, contractors' IR&D portfolios will be smaller and increasingly less technically promising.
>
> DoD negotiators perceive that this is already happening more frequently than it did in the past. As a result, the amount of IR&D performed is reduced and DoD does not have access to the data it sought in the first place.
>
> In many ways, the IR&D cost-recovery process resembles other government programs intended to stimulate private behavior – for example, the investment tax credit to encourage capital investment. We know of no instance of this type of program in which the government takes ownership of the result of the intended private behavior. [15]

General Accounting Office Study of DoD Procurements of Nondevelopmental Items

In a report to the House and Senate Armed Services Committees, the National Security and International Affairs Division of the General Accounting Office (GAO) evaluated DoD efforts to buy off-the-shelf commercial items and other items already in existence (nondevelopmental items, or NDIs). The study noted that one of the major impediments to such purchases was the widespread DoD practice of acquiring and releasing technical data to contractors' competitors.

The report states

> For items that may have potential for profit in the commercial market, industry officials said that the government's practice of obtaining and disseminating technical data to stimulate competitive procurements is short sighted and threatens long-term government and industry interests. For example, prime contractors have cited difficulties in securing subcontractors and increased negotiating time and costs as results of the government's excessive requests for technical data rights.
>
> One industry association official said that almost all commercial products and many other NDI purchased by DoD have already been developed exclusively at the seller's expense. This official and the individual vendors we spoke with said it is extremely inappropriate for DoD to both allow and encourage a competitor to produce a product and make a profit from someone else's original research and development efforts.
>
> It is understandable that industry officials are extremely concerned about providing the government with rights to technical data for commercial products and other NDI that would enable another manufacturer to produce an identical item. Commercial vendors generally told us that they are not in the business of providing a means to support their competition by disclosing proprietary information or surrendering rights to technical data. [16]

Office of Technology Assessment Study of the Defense Industrial Base

The Congress' Office of Technology Assessment, in a recent study of the defense industrial base, found similar results. The office concluded

> In order to motivate diversified subtiers to remain in the defense sector, it will be necessary to make defense work more attractive through changes in acquisition laws, *particularly as they relate to technical data rights claimed by the Government.* [emphasis added] [8]

SURVEYS

Corroborating the impressions and conclusions of these industry contacts, statements, and studies is another body of evidence that comes from industry surveys conducted by DoD institutions and by industry groups. These surveys are summarized as follows.

Naval Postgraduate School Study (Lamm)

Professor David V. Lamm of the Naval Postgraduate School, Monterey, California, mailed a questionnaire in the summer of 1986 to more than 1,300 firms from eight industries, including ship repair, machine tool builders, construction, tooling and machining, electronics, electrical/electronic and communications

equipment, automatic data processing equipment, and aviation equipment. The survey asked respondents to identify their experience with defense business and their attitude toward obtaining defense contracts. A total of 427 firms responded. Almost exactly half of the respondents (213) said that they either did not want defense contracts or had significant problems with defense procurement. In this group that refused DoD business or was seriously dissatisfied, "technical data rights problems" were cited as one of the leading causes of problems 12.6 percent of the time, out of the total of reasons cited.

But if we remember that the major problem that contractors and subcontractors have with DoD's technical data practices is alternative sourcing of whole systems, components, and parts, which has the direct result of cutting contractor profitability or return on investment, then the negative impact of DoD's technical data policy appears significantly larger. "Low profitability" was cited 32.4 percent of the time, and "more attractive commercial ventures" was cited 34.3 percent of the time. The reason cited most often as causing dissatisfaction or refusal to participate in defense business was "burdensome paperwork" (69.0 percent). Yet when contractors explained what they meant by "burdensome paperwork," they claimed, for example, that it was "too much paperwork for 3 to 5 percent profit," or the effort was "not worth the potential return" [17, 18].

Naval Postgraduate School Thesis (Schauber)

Another study took a more focused look at reasons why nonferrous foundry subcontractors refused to participate in DoD business. The study, conducted in 1988, included a survey questionnaire sent to 1,326 nonferrous foundries to obtain information on their attitudes about DoD business. Of this total, 244 responded. The study focused on the 20 percent of respondents who said they were subcontractors that refused, or intended to refuse, to participate in DoD business.

The nonferrous foundry industry was selected because it is critical to both the national economy and to DoD. Nonferrous castings have widespread, critical applications in DoD aerospace, combat vehicle, and naval weapon systems. Virtually the entire domestic output of certain specialized castings, such as titanium castings, is consumed by DoD. The reduced foundry capacity available to DoD is creating longer lead times and higher costs for high-quality nonferrous castings. These longer lead times lead to "bottleneck production delays" in many weapon systems.

Government policymakers and academic researchers often cite the foundry industry as an example of how shrinkage in the defense industrial base is resulting in high cost, long lead times, and lower quality in DoD weapon systems.

The study states

> The increased risks, substantial regulatory requirements and emphasis on price competition in today's DoD marketplace is providing these subcontractors with powerful incentives to pursue commercial vice DoD business. Until these policies change, commercial sales will always appear more attractive, particularly when existing capacity is strained by commercial demand. These forces have caused substantial erosion of the DIB [defense industrial base] in its critical lower tiers. [19]

The survey showed results very similar to those of the more broadly targeted industry study by Lamm. Of the six reasons consistently cited by foundry subcontractors for not participating in DoD business, "more attractive commercial sales to non-DoD prime contractors," was cited by all groups. The report notes, "Commercial sales to non-DoD contractors were universally cited as more profitable and less aggravating." A second reason cited in the top six was "low profitability/lost money on Government related subcontracts." This reason was also consistently cited by all groups. Again the report mentions

> The "real" costs of this paperwork combined with the current emphasis on price competition by the primes and the Government has significantly cut profit margins.... The increasing demands on contractors to fund development programs increasingly place small business subcontractors at risk. Commercial sales are universally believed to be safer and more profitable. In an increasingly competitive international marketplace for castings, each of these factors provides a powerful incentive for a foundry to exit the DoD marketplace in order to avoid these risks, additional costs and "frustrations." [19]

Defense Systems Management College Study

The Defense Systems Management College undertook a study to discover whether or not there was an unacceptable exodus of firms from the defense sector or a marked reluctance on the part of corporations to undertake defense business. The College sent out 831 questionnaires to companies from a cross-section of industries and tiers of the defense industrial base. Received were 244 responses, which were supplemented by approximately 50 personal interviews with company and association executives. The survey asked the companies about their experience in the defense business and their attitudes toward it (for example, did they intend to remain or diminish their involvement?). Twenty-one percent of the respondents said either

they do not want or they intend to diminish or leave defense business. Since respondents also advised the study's authors that fear of retribution by DoD made some of their answers less than candid, the authors state that the true figure is probably higher.

The survey allowed respondents to state in their own words what primary administrative burdens in defense business keep them out of, or are detriments to, DoD contracting. Respondents were also asked to cite changes that would most induce them to enter or get back in the defense business or to increase their role. The authors then grouped responses in categories.

Out of 22 categories, problems with rights in technical data ranked eighth in number of times cited as the first or second most significant problem for the 244 respondents. However, this ranking, again, is extremely deceptive. One of the two primary authors of the study, Lt. Col. David Scribetta, indicated that technical data rights problems were also iuentified or listed as part of other categories of administrative burdens, such as "procurement policies" (rank number 1) and "government attitudes" (rank number 5). He said that many respondents had said technical data issues were a major problem.

Furthermore, when the survey focused on those firms that have dropped out of DoD business or have reduced that business, "procurement policies" (including technical data) were again cited first, with 62 percent of these firms singling out that factor. "Government attitudes" was ranked third, with 36 percent citing that problem. And, very significantly, of the top five factors that were cited by these firms that, if changed, would induce them to come back into defense business, "profitability" and "investment/capitalization" were ranked fourth and fifth, respectively. "Procurement policies" and "Government attitudes" again led that list.

The report itself specifically states that these issues are linked with technical data problems:

> As will be seen over and over again, many of the potential reasons for dissatisfaction are linked. In Table 32, for example, the aerospace industry links the issues of *technical data rights* and *investment/capitalization* [emphasis in original]. There is a significant disagreement between government and industry. Several respondents felt that . . . DoD thinks it is industry's "role" to make these investments. The survival of a firm, however, is often too closely tied to the need for nearer-term profits.

The report also specifically highlights the profitability issue. It states

> Unfortunately for the defense industrial base, for the Department of Defense, profit is a dirty word. Respondents noted that few government personnel understand that, in order to operate, a private firm must make a profit.... Respondent after respondent complained of the attitude within the government that all contractors were criminals, as "proven" by their desire to make a profit.
>
> Profits almost appear as a measuring rod for auditors. Straight contract costs cannot be reduced beyond a certain point. Profit, however, can and the attempt is made to do so without any appreciation for its role in private industry.

The report cites the statement submitted by a large aerospace company, including

> The requirement to give up technical data rights for new technology developments on follow-on contracts discourages companies from making the investment to make these developments. Retention of the technology advantage is necessary to encourage industry to stay in the business, and an opportunity to recover its investment.

The report quotes a large military electronics firm as saying that such policies were

> ... not only a disincentive to contractors ... but also detrimental to the U.S. economy since this places our industries at a major disadvantage in competing with foreign suppliers who are subsidized rather than taxed by their own governments. [20, 21]

Proprietary Industries Association Member Survey (1988)

In addition to the 1991 survey conducted by the Proprietary Industries Association and discussed at the beginning of this chapter, that association conducted an earlier survey of its members also specifically dealing with their perceptions of technical data issues. The survey questionnaire was mailed in the spring of 1988. The 35 member companies that responded unanimously said that then-current DoD policy on technical data discourages (1) vendors' development and use of new technology in products sold to the Government and (2) industry participation in Government procurement. About one-third of the companies had refused to bid on Government contracts or had taken exception to 75 percent of the Government contracts they had negotiated because of technical data rights requirements.

CONCLUSION

An initial question in this investigation must be: Is there a significant problem for DoD as a result of its technical data policies? If there are no serious adverse consequences, either now or for the predictable future, then DoD need not alter its current course. But we believe there *are* significant adverse consequences resulting from the current policies and practices, as the above evidence indicates. If it is not willing to accept these consequences, DoD needs to take action.

CHAPTER 7

COMPETITION

As has been pointed out repeatedly, the conflict between DoD and its contractors and subcontractors with regard to technical data, especially technical data that might appear in a CALS system, derives primarily from DoD's practice of establishing alternative sources to create competition for reprocurement of weapon systems and their components and spare parts. That policy is a principal driver of DoD's need for its contractors' detailed design and manufacturing data. If it did not demand detailed design and manufacturing data, DoD would not have nearly the same degree of conflict with its contractors. It is therefore worth taking a closer look at that policy.

The laws that launched the current fervor for competition were passed by Congress in response to "horror stories" about outrageous spare parts prices being paid by DoD to sole-source suppliers. The assumption underlying these laws is that competition will reduce prices and eliminate the parade of horrors. Were those stories accurate portrayals of pricing abuses in the first place? Were there widespread pricing abuses in excess of, say, those in commercial industry?

Second, does competition actually reduce prices in dual sourcing and in reprocurements of spare parts?

Third, are there adverse consequences to these competitive procurements that need to be balanced against any apparent benefits (such as reduced prices) and that might make these competitions Pyrrhic victories?

THE HORROR STORIES

In the mid-1980s, the tales trumpeted in the press and Congress of wildly excessive pricing of parts were meant to give the impression that there was widespread parts pricing fraud and abuse by industry and that DoD was either in collusion or incompetent. Was that impression accurate? How else could one explain the discoveries of a $435 hammer, a $9,600 Allen wrench, and a $1,500 pair of pliers?

Yes, there were clear instances of abuse. But the amount of abuse was not widespread and probably did not exceed the amount suffered by private corporations in their routine dealings with fellow commercial companies, not all of which are ethical. The most common causes of the high prices were, rather, the following:

- *Line item cost allocation.* Most of the horror stories came from this completely legitimate accounting practice. As an example, let us assume DoD purchased an aircraft spare parts package of 2,000 items for $10 million, which includes support costs of $500,000. One of those 2,000 line items is a landing gear assembly with a cost of $19,000. Another is a Phillips screwdriver with a cost of $4. Under accepted accounting practice, the support costs could be allocated arithmetically across all the 2,000 line items equally. That would give each line item a pro rata support cost allocation of $250. As a result, the landing gear assembly would be shown as costing $19,250. Not unreasonable. The screwdriver would be shown as costing $254. Horror story. Yet the total package price for the spares kit might have been an outrageously good deal. The line item "prices" were basically irrelevant.

- *Small order quantities.* DoD frequently bought spare parts in small quantity orders. As is well known, the unit prices of purchased items can go down dramatically as the volume goes up. For example, a simple diode with a material cost of $.04 each, might cost $110 when ordered in a lot of only two diodes (with general and administrative overhead costs and profit added in). If the same item is bought in a quantity of 100, the price can be reduced to $2.25 apiece. And if bought in a lot of 1,000, the price could be $.27.

- *Overspecification.* The Department of Defense has thousands of extremely complex specifications for fairly simple, commercial-type items. These complex military specifications for common items are a well-known cause of what to a layman would appear to be blatantly outrageous prices [22].

It should be noted that none of these problems – whether fraud, accounting practice, low-quantity orders, or overspecification – can be solved by competition. Yet Congress presumed that the cause of the pricing scandals was sole-source contracting and prescribed mandatory competition as a corrective.

DUAL SOURCING AND COMPETITIVE REPROCUREMENT OF SPARE PARTS

There are two closely related questions in any assessment of the merits of dual sourcing and competitive reprocurement: Does it actually save money? Is the quality the same? Let us first look at the latter of these two issues.

Quality and Technology Transfer

Suppose you want to buy several Cadillacs for your company. After receiving your first several deliveries from one dealer, you accept an offer from another dealer to deliver the remaining Cadillacs at a price significantly lower than that of the first dealer. You accept the new dealer's offer, but when the Cadillacs are delivered, they turn out to be Chevrolets instead. The price is very much reduced from that for the Cadillacs. Have you saved money? You don't know, because the two items are not the same, even though they have roughly the same function. Comparing the two prices is like comparing apples and oranges.

If we assume that the Chevrolets, though perhaps not meeting all of your ideal criteria, are nevertheless satisfactory for your needs, have you saved money? You still don't know, because the Chevrolets, being of lesser quality, will probably wear out faster and need to be replaced more frequently than the Cadillacs. So, over the life of the cars, you may actually spend more money with the poorer-quality-but-cheaper Chevrolets than with the Cadillacs.

This example crudely illustrates a major question that is almost never faced squarely in discussions of the merits of second sourcing, whether it be for production of a complete weapon system or for components or parts of that system. Especially when complex, high-technology systems or parts are involved, there is a very serious question whether a source other than the original manufacturer can produce the same quality item. If the second source does not deliver an equivalent item of equal quality, *one cannot compare their prices; they are different items*! If the second source delivers the lower quality item at a lower price, *it cannot be said that one has saved money*. One does not know whether he has in fact saved anything until the life cycles of the two different items are known. If the item from the second source has a lower mean time between failures, one may in fact spend much more overall on the "cheaper" item than on its "costly" cousin, because it has to be replaced more often. Yet most comparisons of sole-source prices to competitively based prices completely ignore this life-cycle cost/quality factor. Under these circumstances, price comparisons are virtually meaningless.

Are there grounds for suspecting that the quality of second-source-produced items is less than that of the original manufacturer? Where complex items are concerned, yes.

It is impossible to transfer from an original item developer to a second production source all the technical information pertaining to the manufacture of a complex weapon system, using a technical data package alone. As a GAO investigation[1] discovered,

> [T]here can never be enough data, it seems, to achieve effective transfer of technology. . . . [C]raftsman's skills, ingenious processes, "tricks of the trade", and esoteric shop practices cannot be reduced to formal, or indeed informal paper. We are told of a component that several contractors have tried to produce according to engineering drawings and specifications. . . . They were largely unsuccessful. It was learned later that the original developer . . . tapered a cylinder wall along its length from the high to the low tolerance shown on the print. This was a cut-and-try method developed in the shop and perhaps never transmitted to the engineering department. Another trick reported was the use of bacteria free water from a deep artesian well in cleaning electron tubes. Other firms unaware of this peculiarity could not clean the tubes successfully. Such shop methods or "trade secrets" are not revealed in conventional procurement data. [23]

Even if a complete, error-free technical data package could be provided to a second source, the problem with complex weapon systems is that they are in constant change, even well into production. The transition from development to production is difficult, even for the original developer, under the best of circumstances. Although concurrent engineering will ease the transition to production, transferring a developer's technology to a second source will still magnify the difficulty enormously. Normally, for transfer to take place, the design of the system has to be very mature and stable. But at that point, well into the production of the system, there are often not enough units left to justify the tremendous costs of establishing a second source. As explained by then-Deputy Under Secretary of Defense for Research and Engineering (Acquisition Policy) Dale W. Church to the House Committee on Appropriations,[2]

> The reason I mentioned validated data packages is that their development typically takes four to five years. If you wait four or five years from the start of production to go into competition with a second source, you have built so many units that there is not enough left for the second source. . . . [T]here is a certain amount of continuous change that occurs in a program, even when the program is somewhat mature in the production phase. You keep getting design changes. [23]

---

[1]General Accounting Office, *Evaluation of Two Proposed Methods for Enhancing Competition in Weapon System Procurement*, Comp. Gen. Rpt. No. B-39995 (July 14, 1969).

[2]*Acquisition Policies, Procedures and Practices: Hearings on Department of Defense Appropriations Before the Subcommittee of the House Committee on Appropriations*, 96th Cong., 2d Sess. 381-2, 1981.

So, for example, the C-141 aircraft had generated 22,500 engineering drawings for the first five aircraft produced. By 2 years later, there had been 21,516 revisions in those drawings, and revisions were running 2,000 per month [23].[3]

Another difficulty is noted by the authors of a Defense Systems Management College handbook for program managers on establishing competitive production sources:

> Given the complexity of modern weapon systems, it may be difficult to document weapon system technology strictly through drawings. Even when drawings are complete and accurate, technological differences between the two companies' manufacturing methods may preclude the second source from manufacturing strictly from the TDP [technical data package]. . . . This may result in later logistics complications if the two designs are significantly different. [24]

In other words, when we essentially end up with two different items instead of one being deployed into the field, the entire logistics system is burdened with the increased costs of supporting two items, not one. After studying dual-sourced ship acquisitions, one investigation[4] concluded that it is impossible to get truly identical end items and that this impossibility will seriously affect their support:

> Even if all systems and subsystems were identical in the two ships, methods of fabrication at the two shipyards would generate differences in the final product. . . . The long-term effect of having two classes of ships in every program that is dual sourced will not be felt until years after they are in the fleet being supplied and maintained to different configurations. [25]

And yet, as we have noted, commercial firms often license others to produce their sophisticated products. Some industries, such as the U.S. aerospace industry, actively engage in transfers of technology. Airframes, aircraft engines, and accessories have all been produced by firms that did not initially develop them. As one study[5] noted:

> Aerospace firms have accumulated vast experience in the art of transferring technology necessary for the manufacture of sophisticated aerospace equipment. Practically every important aerospace firm in the world has served as a licensor or licensee in at least one of these programs. A number of firms have been involved in both capacities; licensor of technology in some programs, recipient in others. [23]

---

[3]R. Johnson and J. McKie, *Competition in the Reprocurement Process*, 1968.

[4]Robinson and Sullivan, *An Evaluation of Dual Source Competition in Ship Acquisition Programs*, Industrial College of the Armed Forces, March 1986.

[5]Johnson and McKie, *op cit.*

What then accounts for the failure to transfer the necessary technology in some instances and the success in others? Two things distinguish the successful from the unsuccessful cases cited above: technical assistance and mutual beneficiality. When aerospace firms transfer their own technology elsewhere, they not only deliver the necessary technical data, they provide extensive technical assistance and assistance in obtaining production materials, production equipment, training of personnel, plant layout planning, and more. As one investigator[6] noted, the requirements for successful technology transfer are as follows:

> Production know-how and assistance made available under licensing agreements includes information, materials and services of the following types: (1) specifications, designs, and productions techniques; (2) planning and construction of plant facilities; (3) purchase and installation of machinery and equipment; (4) training of licensee personnel; (5) adaptation of products and production techniques; and (6) engineering and consultation services and advice. [23]

The other necessary condition for such transfers to take place successfully is that the arrangement be mutually beneficial. Commercial firms do not engage in such technology transfers if it does not make business sense for them to do so. These are voluntary, mutually beneficial actions. So, as noted in Appendix C, for example, a firm may license its older technology to provide income from the royalties as a source of funds for developing future technologies. Or a company may agree to license another firm to make a component toward the end of a production run when the licensee can make the component more cheaply, the licensor can receive a good royalty, and the buyer can receive a lower price for the component. These transfers are done face-to-face between the source company and the recipient of the technology (the second source). The buyer need not be involved in the transfer.

In contrast, when a company is forced to give up critical advanced technology to establish a second source in an arrangement clearly inimical to its interests – and when that transfer, by necessity, is made by means of technical data alone without the cooperation of the original source – the transfer, at least for complex items, is unlikely to be successful. Then one is faced with the problems of lower quality or nonidentical items generated by the second source, as mentioned above. Even if this cooperation is made a condition of the original production contract with an original source, one must question whether that cooperation will be truly effective when it is not in the source firm's interest. On the other hand, for simple parts having many

---

[6] *Ibid.*

existing or potential suppliers, there is little or no quality risk in buying from an alternative supplier.

When is an item, component, or part so complex that it should not be reprocured from a second source by using technical data alone without the full cooperation of the original source? This matter obviously calls for a subjective judgment, but perhaps a working rule of thumb might be: Whenever a part cannot be manufactured by a second source on the basis of form, fit, and function data and standard industry manufacturing processes and specifications, then establishment of a second source will require the original source's genuine cooperation. In such a circumstance, if second sourcing continues to be required, development of the additional source should be left to the original source through private means, such as direct licensing. To put the rule in other words, if detailed design and manufacturing data are required, so is the cooperation of the original source. Lacking that cooperation, one cannot successfully transfer the technology. This rule of thumb is conservative; some parts and components can be made to the same quality standard by other than the original manufacturer, when the second source is given detailed design data and has roughly comparable experience, appropriate tooling, and other necessary equipment. But the risks of reduced quality go up significantly at this level of part complexity. And, though conservative, the rule would balance economic and technical concerns better than the current practice does.

COSTS AND SAVINGS IN COMPETITION

If we ignore the issue of variations in quality between an original source's item and one produced by an alternative source, can we say with confidence that competition produces improved prices for DoD in its procurements of weapon systems, components, and spare parts? Economic theory would suggest that it does. We have already alluded to the fact that high-technology companies try to keep their latest and best technologies secret so that they can extend their monopoly positions longer and thereby charge higher prices (sometimes called "monopoly rents") that help them to recoup their past development investments, capitalize their future development, and make a profit commensurate with the risks assumed. To a large degree, it is the taking away of these higher monopoly prices through competitive reprocurement that causes industry protest. When, in addition, the establishment of second sources is accomplished by giving those sources the original company's most sensitive technical data, thereby at least potentially enabling the second source to cut

into the original company's *commercial* markets as well as defense business, the protest becomes a howl.

In 1965, then-Secretary of Defense Robert S. McNamara testified to the Joint Economic Committee that introducing competition into a sole-source procurement situation usually produced savings of at least 25 percent [26, 27].[7] In the ensuing years, that number, 25 percent, has been quoted regularly by defense policymakers and observers. In the current DoD regulation governing the procedures for spare parts breakout, when the costs and potential benefits for a candidate competitive reprocurement are calculated, the life-cycle savings factor assumed to result from competition is 25 percent.[8] Does competition in reality produce these savings in dual-source production? In competitive reprocurement of spare parts?

Dual Sourcing in Weapon System Production

In the 1970s, four studies of major weapon system acquisitions seemed to confirm these savings from introducing competition in production. The studies have subsequently been cited regularly as evidence of significant savings. But more recent investigators have challenged both the methodology of these studies and their conclusions.

The early studies were weak in a number of significant ways. For example, the systems analyzed were not representative of major defense acquisitions but instead consisted of inexpensive electronic or electrical components, guided missiles, or munitions. In addition, the studies calculated the unit costs from the sole-source supplier on the basis of either no production experience or minimal, early experience. And the data often included nonrecurring start-up costs for developing the system and establishing the initial production line but not for establishing the second source. These errors artificially inflated the early price levels of the original source, which were then projected out to the end of production. Comparing the subsequent prices, after competition was introduced, to these artificially inflated sole-source prices yielded the estimates of savings [27].

The consensus of recent investigators from DoD, academia, private firms, and Federal investigative organizations is that dual sourcing of complex systems and

---

[7]Benjamin R. Sellers, "Second Sourcing: A Way to Enhance Production Competition," *Program Manager*, Vol. 12 (May–June 1983), p. 12.

[8]DFARS Supplement No. 6, *DoD Spare Parts Breakout Program*, 25 November 1988.

major components is just as apt to result in higher production costs as in lower ones, while overall costs will most likely be significantly higher. And even the effect of *threatened* competition, sometimes cited as controlling or even reducing costs, is unclear [27]. See, for example, the following analyses:

- Stephen Miller [25], who identifies one of the major problems with split production awards (giving the low bidder most of the units for production and the second bidder the remaining units, often in a 60-40 split) as follows: This method does not engender true competition. Although it assumes that both bidders will actively compete in price for the larger portion of production, this is not necessarily the case. Rather, since the losing bidder is guaranteed at least the smaller award, it may find it more profitable to bid a very high price and produce the smaller quantity at that price. And if, by chance, it wins the larger portion, it receives a windfall. In either case, the Government pays a premium.

- Donald Pilling [27], who concludes

> Drastic cost-cutting actions by major aerospace contractors, which win contracts but which also mortgage the contractors' future capabilities, are not in the government's best interests if a broad and modern defense industrial base is desired. A partial solution to this dilemma has been to keep two competitors going with production of the same item. The contracts give each firm the resources it needs to sustain modern manufacturing capabilities and current engineering expertise. Although the competitive environment may offset some of the additional cost of carrying two contractors, little evidence exists that dual sourcing actually reduces program costs. Indeed, data . . . suggest that a split purchase is more likely to increase the costs for a project.

- Joseph F. Grosson and Joseph H. Augusta, "Cost of Competition and Its Consideration in the Acquisition Strategy," *Program Manager*, 15: 33-36 (July – August 1986), cited in Miller [25].

- Michael N. Beltramo, "Findings and Thoughts About Competition in the Procurement of Weapon Systems," *The Journal of Cost Analysis*. 4: 1-12 (Fall 1986) cited in Miller [25], who found that of 25 systems studied, only 6 showed a decrease in price compared to the sole-source price, whereas 12 systems showed price increases.

- Karen W. Tyson, J. Richard Nelson, Neang I. Om, and Paul R. Palmer, who conclude

> Dual-source production should not be prescribed across the board for major systems. Competition can be of value in particular individual cases; however, it is very difficult to predict what those cases are. Additional work needs to be done on criteria for competition. It should not be universally applied. The larger and more customized the system, and the lower the quantity, the harder it is for competition to be viable because of the larger

investment. . . . That cost savings from competition are uncertain should be recognized. [28]

- Kemal Guler and Charles R. Plott, who found that whereas the normal methodology used to compare prices before and after competition in production (criticized above) predicts savings of up to 30 percent from competition, in fact, using actual average costs obtained under sole sourcing over the course of a program leads to the conclusion that second sourcing *increases* procurement cost by over 40 percent on average [29].

Boger, Greer, and Liao [26], summarizing the latest conclusions, state: "With the improvement in research methodologies, studies conducted in recent years revealed that competition has resulted in *added* net costs almost as often as it has produced the desired net savings."

In accordance with the pessimistic conclusions of these and other studies, dual sourcing as a means of reducing the costs of weapon programs seems to be going out of favor somewhat in DoD and perhaps with Congress as well. (See for example the statutory change in the FY91 Defense Authorization Act, discussed in Chapter 2 and Appendix A, eliminating the presumption in favor of dual sourcing in production of major systems.) This perhaps is also due in large part to current reductions in Defense budgets, which have drastically reduced the number of units affordable for almost all new weapon system acquisitions. With the lower volume of production, dual sourcing clearly becomes economically infeasible. But what about competition for spares?

Competitive Reprocurement of Spare Parts and Components

Dual sourcing of weapon systems in production is one instance in which DoD takes an original source's detailed design and manufacturing data and transfers them to another company as a second source. The other major such transfer of the data by DoD is for the competitive reprocurement of spare parts and components. The focus here is not on very simple, standard parts with many existing vendors. For the purposes of this inquiry, our focus is only on the establishment of second sources for items unique to a particular company that require the use by the second source of that original company's proprietary design and manufacturing data.

In assessments of the value of competition for spare parts and components, for the most complex items we might expect to find results similar to those identified

above for major systems and subsystems. Or do we find the presumed 25 percent savings?

There are not too many studies that directly address this narrow range of circumstances – transfer of sensitive spare parts product data to an alternative supplier – although some of the studies of dual sourcing allude to it. A GAO study conducted in 1984 evaluated prices for a broad range of products before and after competition, including spare parts and components as well as major systems. For the overall universe of competitively procured items evaluated, GAO concluded

> [D]ual source procurement solely for production price competition can be cost effective only when the product price reduction resulting from competition outweighs all costs to the government for establishing and maintaining the additional source. The major problem is identifying such procurements when faced with uncertainties about their future. . . . GAO believes guidance and the employment of case-by-case cost/benefit analyses are essential to an agency's determination of the savings likely to be achieved through dual source procurement. However, this does not eliminate GAO's underlying concern that dual source procurement's overall cost effectiveness is uncertain. The cost savings validity of the production dual source concept is unknown. [30]

As GAO noted in its report, in order to assess whether there have been any savings as a result of competition, we need to know what all the program costs were. In a recent DoD Inspector General audit, the IG concluded that the "Military Departments and the Defense Logistics Agency were unable to accurately determine the cost-effectiveness of their Spare Parts Breakout Programs" because they had no uniform and accurate way to calculate their program costs. Nevertheless, DoD had reported to Congress that significant savings had resulted from the breakout program. It must be noted that the breakout program includes the alternative of procuring spare parts from the actual subcontractor-manufacturer of a part rather than from the prime contractor, thereby avoiding the prime's markup of costs. This aspect of the program is of no interest in our inquiry, because it does not involve taking sensitive data away from the originator of the data. It is only the competitive reprocurement from other than the originator of the data that is our concern. It is not clear how much of DoD's reported savings came from breakout to the actual manufacturer.

The IG found that total actual costs, although necessary to calculate any savings or net loss, could not be accumulated because the necessary accounting system to capture actual costs did not exist. Nor were there any specific guidelines on

which costs to accumulate. Some of the Service organizations did not include labor fringe benefit costs or other direct operating expenses. None of the organizations reported indirect costs, such as administrative and personnel support automatic data processing, security, office space, and utilities. Interestingly, when the IG calculated savings that might have been recovered if the agencies had avoided certain identified errors, the IG used the 25 percent rate of savings assumed for competition in DFARS Supplement No. 6 [31].

In addition, other costs associated with these procedures for competitive procurement are ignored altogether, such as the increased lead time for procurement. For example, the time it took to buy a part increased from about 60 days in 1982 to 150 days in 1986 [32].

We are left with a picture that is unclear at best. There is no hard evidence at hand to support – or contradict – assertions that competitive buying of complex spare parts saves money. This is a very different picture from one that assumes that such competition routinely saves 25 percent in comparison to buying from the original source alone.

OTHER ADVERSE CONSEQUENCES

We have already mentioned the risk of lower quality in complex parts that are not procured from the original manufacturer. There is also the risk that the part, though of high quality, may simply be different enough to place additional strain on the supporting logistics system. There are two other potential adverse consequences worth specifically highlighting.

In the Guler and Plott California Institute of Technology experimental study [29] cited above, the researchers identified three additional effects independent of the 40 percent increased overall cost of second sourcing. These effects apply when potential commercial markets are rendered vulnerable by the private developer's contract requirement to surrender proprietary technical data for possible second sourcing by DoD:

> 1. Contract winners anticipate that their profits will be lower in the future and invest less in research and development (R&D) than under sole-source conditions;

> 2. The prospect of reduced future return causes every bidder to bid less aggressively in the initial procurement phase than under sole-source conditions; and
>
> 3. Sellers with commercial markets that may be adversely affected by data rights provisions completely drop out of the bidding in the first phase if the value of [their] commercial operations is high relative to the profit they expect in the procurement market. This results in fewer bidders in the initial phase and higher initial period procurement costs on average. [3]

These results essentially corroborate the results we have already identified. Defense contractors, and especially critical lower tier subcontractors, are dropping out of defense business, not bidding in particular major programs, and withholding their best technologies from DoD programs out of concern for the loss of markets and the lack of real return for their allocation of scarce corporate resources. This is a very powerful counter argument to those who express the view that second sourcing, whether for major systems or parts and components, expands the defense industrial base. In fact, when second sourcing requires exposure of contractors' sensitive data to potential competitors (even with restrictions on further use, such as with GPLR), it tends in the opposite direction.

A second set of problems is associated with the legal liabilities of second sourcing. As was noted by one commentator[9]

> Historically, contractors have blamed their failures on data furnished by the Government whether such data was generated in Government laboratories or in the developing or producing contractor's organization. Under these circumstances the Government has contracted for, reviewed and policed furnished data. . . . The Government serves in the role of middleman . . . between two contractors each blaming the other and the Government for failure to produce. [23]

The second source can fall back on the technical data given to it as the cause of any failure to perform and may allege extra costs required to correct deficiencies in manufacturing inherent in using the data [23].

THE SURGE/MOBILIZATION JUSTIFICATION

In addition to price control, competition in production is justified as a means of increasing the number of potential suppliers available in the event of an emergency to increase production volumes suddenly (surge or mobilization requirements).

---

[9]Armed Services Procurement Regulation Committee Case 69-95.

This justification is also questionable. First, as already noted, the competition policy, especially when proprietary technical design and manufacturing data are used, is causing contractors and subcontractors to abandon the defense industrial base. It thus has an effect just the opposite of the one intended – it reduces the number of suppliers rather than increasing it. Whether these suppliers are then replaced by equally qualified substitutes equally ready to perform the defense work is unclear, but doubtful. The surveys suggest that, in critical areas of the subcontractor tiers, genuine and significant attrition is occurring [27].

Second, this justification seems plausible only when the original contractor cannot satisfy DoD that it can meet surge/mobilization needs when they arise. It would be an unusual circumstance, however, when a contractor would not be able to expand production – for instance by hiring additional workers; by going to additional work shifts; by building additional, idle capacity (at Government expense); or by licensing additional sources itself – at least as well as several sources having to do all these things at the same time but in smaller amounts could. The surge or mobilization need would be for the current production, regardless of how many sources are producing it, to expand rapidly to an enhanced level. If that expansion is to take place by hiring more workers or multiplying the work shifts, usually that can be done at a single plant with a large production capacity at least as easily as at several plants with small capacities. If that expansion is to take place by investing in prior, idle capacity, usually that can be done more easily at one plant with larger reserved capacity than at several plants with small reserved capacities. And if that expansion is to be accomplished by suddenly starting up other sources through license or other arrangements, that must be accomplished by the source firm.

SUMMARY

To recapitulate, DoD and Congress have adopted a policy of competition for production of weapon systems and their components and spare parts as the primary tool to attack what are seen as high costs. Whether competition actually produces lower costs, especially for complex, high-technology items and components, is very questionable. Most recent analysts have concluded that over the life cycle of the item or component *higher*, not lower, actual costs are equally or more likely to result. Furthermore, the more complex the part or item, the more likely it is that the second-source production will yield a lower quality item, or at best an item with enough difference from the original to require extra support costs. These additional costs can

be substantial over the life of a system. Finally, the policy has other widely identified adverse results, such as additional attrition of the defense industrial base (resulting in weapon systems of lower quality and, perhaps, higher prices due to lack of effective competition). With regard to justifying competitive sources as a means to provide for emergency rapid expansion of production, this rationale would seem defensible only when the original source cannot provide DoD with a credible plan to meet that need when it arises. This is likely to be a highly unusual case.

The competition policy, as executed by DoD, is primarily designed to get lower *absolute* prices. The assumption is that higher prices are "unfair" or "unreasonable." But, as we have noted, "higher" prices may actually represent the minimum price necessary for a producer to recoup research costs, invest in future research, and yield a reasonable profit for the risk assumed. A foreign manufacturer trying to sell its product in the United States below its real costs of doing business would be accused of "dumping" that product and could be subject to severe economic sanctions. The same principle should apply in the DoD marketplace: price should not be considered unreasonable if it represents the real costs of doing business plus a fair profit. The consensus of recent analysis seems to be that DoD is arbitrarily trying to force sellers to stay below this fair price level by competing prices at each stage of the life cycle of the weapon system, including development, production, and support. In today's world, excellent companies with other markets in which to sell their excellence will abandon a monopsonist customer that insists on these conditions of business.

The policy of competition causes DoD to demand its suppliers' design and manufacturing process data, to write its procurement rules in a way that captures the data to the maximum extent possible, and to adopt aggressive practices aimed at getting the data from all levels of suppliers. Demanding the data has generated tremendous conflict with defense suppliers and potential suppliers. A very fair question, at least with regard to the policy of competitive sourcing in production and support, is: Is it worth it?

CHAPTER 8

RECOMMENDATIONS AND ALTERNATIVE SOLUTIONS

In keeping with the charter for this study, we have identified several sets of possible solutions to the significant industry concerns identified in Chapters 1 through 7. These sets of solutions are intended to indicate areas that are good candidates for further development. We will address first those recommendations specifically related to issues of CALS implementation and then discuss recommendations aimed at the underlying technical data issues.

CALS SYSTEM SECURITY

Recommendation 1: Revise current concepts for implementation of CALS Phase II.

In our contacts with prime contractor, subcontractor, and DoD officials, the near-universal assessment was that CALS as currently envisioned for Phase II will simply not be supported by industry. At lower tiers of the defense contracting community, the antipathy is expressed more vehemently: These subcontractors say they simply will not participate in DoD programs subject to such an open data architecture, period. The risk of exposure of their most sensitive technical data, as well as all the other dangers we have discussed, are simply too great. Contractors believe that the CALS Phase II concept as currently envisioned would result in de facto delivery of their sensitive proprietary data, regardless of what may be the delivery requirements of their contracts.

The following proposals address aspects of data security in a CALS system. They deal with the security of technical data required to be delivered to the Government. They do not, however, solve or address the underlying issues of what data must, by rule and contract, be delivered to the Government and the uses that can be made of that data. The security alternatives, which may be employed individually or in combination, include:

Alternative 1. Separate, discrete data base for integrated weapon system data. Instead of the proposed CALS Phase II CITIS/IWSDB concept of shared data bases

(using the contractor's corporate data base with DoD access to a portion of that data base), a separate data base could be established for weapon system technical data. Contractors would enter data into this data base only as required under their contracts and only when release of the data has gone through internal corporate review and approval.

The discrete data base would still enable users to have instantaneous access to all needed data. Thus the primary goal of CALS would be met, while industry fears over unauthorized access to corporate data would be allayed. Although a separate data base would impose an additional cost compared to direct access into a contractor's working corporate data base, it would probably not impose any more cost than would be required to institute the access and other security controls that would be necessary in the envisioned shared data base concept. Furthermore, the security controls available for the foreseeable future that would be necessary in a shared data base concept would probably inhibit the use of the total network to such a degree that the original concept could not be implemented anyway.

Alternative 2. Incremental implementation with confidence-building. CALS Phase II data bases can be implemented in a stepped manner, beginning with a system that incorporates only nonsensitive corporate technical data. As the security of technical data in the system is proved to the satisfaction of industry, more sensitive data can be incorporated into the data bases. The system would grow in step with companies' confidence in its capability to protect their most critical data.[1]

Alternative 3. One-time, multisite log-ins. One of the principal industry fears about the current vision for Phase II is the idea that firms will lose control over who has access to their data. In a paper-based technical data system, a contractor is required to log in to multiple data repositories in order to gain access to all the needed data. Thus, the user has to pass through a series of hurdles or barriers making unauthorized access and use of data extremely difficult. But the CALS concept envisions that only one log-in would be performed. What if a mistake is made at that

---

[1]Having separate CITIS data bases as proposed in Alternative 1 above would help solve the problem of protecting data from external users, but it would not solve the problems of data aggregation and "browsing." These problems are present in CITIS levels three and four ("Ad Hoc Queries" and "Applications," respectively). Contractors should not be required to establish those levels until both DoD and the contractor are satisfied that adequate controls are in place to protect the integrity of the data.

log-in, and an unauthorized user is instantly granted access to sensitive contractor data?

One possible correction to this problem might be to require that requests for access to data residing in multiple locations, as with the CITIS concept, be instantly forwarded to *all* the sites containing requested data. Each CITIS contractor would have an opportunity to review and challenge the request. Controls on abuse of this process, such as time limits on the right to challenge, would, of course, also have to be implemented.

Alternative 4. Multilevel access controls. Numerous proposals have been made to incorporate multilevel access controls similar to those employed in national security classified systems. There are available commercial systems that provide roughly comparable security. There are many problems with such a concept, however.

First, it is almost impossible to imagine the CALS concept working if classified data are included in the weapon system data base. Classified systems work almost exactly opposite to the CALS concept. For example, they usually require dedicated communications lines rather than using normal, open commercial networks. And data delivered into a classified automated system environment are not allowed to go back out of that environment in electronic form. They can be taken out of the classified environment in paper form only, with very tight security controls. Information does not flow electronically in two directions, only one.

Another problem is the personnel turbulence in industry. A person who is working for one contractor one day, with security clearance for that contractor, may the next day be working for a competitor. It is difficult to imagine an adequate and cost-effective system of controls over personnel clearances that would protect against possible abuse and in which contractors would have confidence.

The degree of controls that would be necessary to ensure safety of data at multilevels of use, sensitivity, and access by such a broad array of potential users would be so inhibiting to use and costly to manage that it would probably shut down the very benefits of accessibility that CALS was meant to provide.

TECHNICAL DATA POLICY ALTERNATIVES

By themselves, however, the above CALS changes are not enough. As long as contractors are required to deliver data that they regard as vital to their economic health into a computer-based system allowing widespread access by potential competitors, they will regard that system as inherently threatening to their vital interests. Thus, unless the longstanding conflicts over DoD technical data policies requiring delivery of sensitive contractor data are satisfactorily addressed, contractors will not fully support a CALS-type system. DoD technical data policy and CALS data security issues must both be satisfactorily addressed before CALS implementation can proceed with a high degree of industry support and cooperation. Therefore, we recommend that DoD consider the following data rights policy changes.

Recommendation 2: Once a major system's production contractor has been competitively selected, DoD should abandon the routine use of subsequent re-competition for production of systems, components, and complex spare parts.

Our entire analysis leads to a conclusion that competing production of systems and spare parts can be counterproductive. We believe that DoD should make a radical turn away from its current policies and practices that routinely embrace alternative sourcing in production and complex spare parts support for weapon systems. The justifications for those policies and practices are very weak and the costs, in overall price and quality, are high. This is especially true as quantities of production items decrease. Eliminating or radically reducing current practice (and the policies that support them) will dramatically improve DoD's business relationships with its suppliers and will enhance DoD's ability to perform its missions by improving the quality and breadth of the industrial base of suppliers offering their best capabilities in DoD weapon systems programs.

Alternative sourcing should be used only in the most unusual circumstances, such as when the original source refuses to present an adequate proposal to meet surge requirements. Alternative sourcing, we believe, should not routinely be used as a mechanism to influence price.

We recognize that implementing this recommendation requires a policy decision at high levels of DoD. But the alternative sourcing practice and demand for contractors' design and manufacturing data lie at the heart of the conflict between

DoD and industry over data rights. And as we have indicated, DoD pays an extraordinary price in adverse consequences as a result of that conflict and CALS implementation is directly threatened because of it.

Recommendation 3: As much as possible, DoD should incorporate spares pricing competition as part of the overall production contract with the original source.

There are two very different goals associated with the pricing considerations that drive the practice of second sourcing, whether for system production or reprocurement of spare parts. As we have noted, there is the quest for the absolute lowest prices, and there is a quest for price reasonableness.

Trying to get the very lowest possible prices for an item, as we have indicated, can be a self-defeating effort. Not only can it actually result in higher overall costs for the life cycle of the item, but it can cause other highly damaging effects, such as a deterioration in the extent and quality of the industrial base and in the quality of technologies being incorporated into critical weapon systems.

But a completely different issue involves how to determine a *fair* price, as opposed to the lowest possible price. The horror stories that launched the latest wave of reforms were exaggerations of the fairness question. The reformers concluded that the only valid way to determine that DoD was getting a fair price was through competition. If there was competition, the reformers believed, then by definition the prices must be fair and reasonable.

There are really, then, two aspects to the price reasonableness issue. The first is determining what price is, in fact, reasonable given the business economics of a particular acquisition. The second is being able to defend that price to critical outsiders, such as Congress and the public. Competition is convenient because it arbitrarily satisfies both needs. It is possible to continue to use competition as a way of ensuring and defending price reasonableness.

Almost nobody objects to competition for development of a weapon system and for the contract award for production of the system (winner takes all). It is the introduction of competition during production (dual sourcing) and for complex, proprietary parts and components that causes industry objection. One approach, then, is to rely on competition at an earlier stage of acquisition to cover a longer

portion of the life cycle of a system. Alternatives might include the following, or some combination of these:

Alternative 1. Extensive initial provisioning competed as part of the production contract award. DoD fields its systems with an initial stock of spare parts. DoD might employ greater one-time, up-front buys of parts stocks sufficient to support the system well into its projected life. If this parts provisioning were competed as part of the production competition, the parts prices could be defended as fair and reasonable because they were established as part of the overall competition. This, of course, would require much higher funding committed at this earlier stage of the program. And it may raise storage costs. But the contractor may offset some of this with lower prices in exchange for the stability, volume, and continued protection for its sensitive technical data. The contractor would (1) be able to keep its competition-sensitive data and (2) be free of the threat of a second source that might endanger its defense and commercial markets. A variation of this would be to include priced options for spares, perhaps with an escalation factor, competed as part of the initial production contract.

Alternative 2. A production contract with a long period of contractor support. In this case, the base contract would include a commitment by the contractor to support the item for a fixed number of years. Award, as in Alternative 1 above, would again be based on the best total package offered. DoD would again get replacement parts support at a price based on open competition, and the contractor would be able to keep its sensitive data. The Army negotiated this kind of contract for its mobile subscriber equipment program (mobile phones). The contractor committed to 15 years of support to the equipment.

Alternative 3. A production contract with a fixed period of spares pricing followed by contractor option. As with the other options, this would incorporate spares prices as part of the competition for system production. In this case, offerors would include a price for spares in their proposals for production. The pricing could include annual adjustments for inflation or other agreed-upon factors. The pricing period could be for a fixed period such as 3 to 5 years. Technical data sufficient to establish alternative sources would be placed in escrow. At the expiration of the initial support period, the continued spares support prices could be renegotiated. If agreement on continued prices cannot be reached, the issue might first go to a disinterested third party thoroughly familiar with the economics of the contractor's

industry and DoD's need, for arbitration or mediation to determine what prices are reasonable under the circumstances. The parties could continue in the contract for a pre-set period of years, such as 2 years, according to the pricing formula set in arbitration. At the conclusion of this period, if renegotiation is again unsuccessful, the Government would have the right of access to the escrowed data in order to establish alternative sources of supply. Further contractor protection could be afforded if the contractor is willing to establish the second source(s) itself under direct license.

The Government would, of course, also have the right to data if the contract is terminated for failure to perform, poor quality, or delivery problems. Obviously, there are many potential arrangements that could be devised in this class of contracts. The fundamental principle would be that DoD gets a competitively based support price for a reasonable period of time and the contractor would be able to keep secure its sensitive data.

Recommendation 4: DoD should consider adopting a policy of permitting contractor nondelivery of proprietary, sensitive technical data, with protection to DoD through third-party escrow of the data or "march-in" rights to contractor-stored data.

As noted, the primary reason why DoD requires its suppliers' design data and manufacturing data is to establish additional sources for the items. The primary reason DoD establishes these additional sources is to introduce price competition for the item with the goal of reducing prices. A secondary reason is to provide for surge and mobilization needs. We have recommended that the practice of routine alternative sourcing be generally abandoned, except when the original source cannot provide DoD with a reasonable surge/mobilization plan.

But secondary reasons for DoD to demand delivery of such data include

- *Security of supply.* Some DoD personnel assert that the agency needs to be able to establish new sources in the event that the original contractor goes bankrupt or otherwise can no longer perform the contract.
- *Emergency repair and overhaul.* As we have noted, sometimes detailed design and manufacturing process data are needed to perform emergency major repair or overhaul of systems, such as ships.

Neither of these justifications actually require physical delivery by the contractor and physical possession by DoD of design and manufacturing data. What they do require is that DoD have guaranteed access to and use of that data *when the actual need occurs.* This requirement can be met by having the contractor deliver the data into a third-party escrow, with DoD having the right (1) of inspection to guarantee that the data are current, complete, and fit for the intended purpose and (2) to enter and take possession of the data upon the happening of stipulated circumstances. An alternative might be to allow the data to reside with the contractor but isolated from routine DoD access with march-in rights for DoD to have access under the given conditions. This alternative would receive much greater contractor support, for as we have noted, contractors are extremely reluctant to let their sensitive data leave their own company, even to be placed in an escrow.

The escrow concept might also be applied in circumstances in which DoD becomes uncertain as to a contractor's future ability to meet surge/mobilization requirements.

If alternative sourcing is not pursued, and if security of supply and emergency repair needs are protected through escrow provisions, there are no remaining strong reasons for DoD to require delivery of design and manufacturing data, *regardless of who funded their development or what rights DoD has in them.*

Recommendation 5: DoD should consider adopting a policy of seeking independent third-party arbitration for price reasonableness determinations before establishing alternative sources.

As discussed under Recommendation 3, the key issue from DoD's perspective in reprocurements from an original, sole-source supplier is price reasonableness. DoD does not want to be stuck with a sole-source supplier that takes advantage of its monopoly position to charge exorbitant prices. We have also noted, however, that the lowest possible price may not be a fair price. And good suppliers will not continue to do business with DoD if they are not able to receive a fair price for their work.

We have discussed the possibility of including more spare part price competition as part of the competition for the original manufacturing contract. But whether or not such price competition is adopted, the issue of price reasonableness for spare parts may appear at some point during the support phase of the weapon system. When there is a dispute over the reasonableness of price for spare parts, rather than

immediately breaking out the parts for competitive reprocurement – with the consequent conflict with original suppliers – DoD could adopt a policy of requiring delivery into escrow of technical data sufficient to establish alternative sources with the original production contract. Then, if DoD later concludes that subsequent spare part pricing has become unreasonably high, the first step would be to seek an independent third-party assessment (identified in the original contract) of the reasonableness of the price, given the underlying economic factors. The parties would agree to abide by the decision of the arbitrator for some period. At the end of that period, DoD would have the option of continuing with the original contractor or having the technical data delivered from escrow and establishing new sources (as discussed under Recommendation 3, Alternative 3).

This option would protect suppliers from arbitrary price-driven action on the part of DoD, and they would get to keep their most sensitive data. From DoD's perspective, the fact that the data necessary to establish alternative sources are eventually available to DoD should provide a strong incentive to the original supplier to keep prices down throughout the performance of the contract. And DoD can introduce competitive pricing with only a minor interim delay to abide by an independent arbitrator's price.

Recommendation 6: DoD should revise the DFARS rights in technical data rules.

Clearly, a major thrust of this study is that DoD should make a radical turn away from its current policies and practices that enthusiastically embrace second sourcing in production and complex spare parts support for weapon systems. If such a policy shift were to take place, the regulations governing rights in technical data and technical data delivery requirements could be revised significantly. We think such a shift would create a much healthier working environment for both DoD and industry and would *enhance* national security and the ability of DoD to perform its missions.

But even without such a shift, there are aspects of the current rules that are a source of unnecessary conflict between DoD and its contractors and subcontractors. These, at a minimum, should be revised, simply for clarity and fundamental fairness.

Revision 1. Clarifying rights in the products of research and development. The current DoD regulations give DoD unlimited rights in technical data resulting from all R&D work. As we have discussed, there is a very significant difference between

(1) research and development that is conducted solely for the purpose of increasing knowledge and the nation's technological base and (2) research and development that has as its purpose the eventual development or potential development of a product for DoD inventory. There is not a significant conflict over the first type of effort. The regulations, the standard contract clauses, and the contracts themselves should make a clear distinction between these two types of effort. Where the first category of R&D is concerned, offerors should be put on clear notice that the end purpose of the effort is to disseminate the resulting new knowledge for the general benefit of the public or scientific community, and that as a result DoD will *fully fund* the research and will take unlimited rights in the resulting data.

Where the second category of R&D is concerned, this end purpose, too, must be clearly announced in the solicitation and contract, and the regulations and contracts must clearly protect the proprietary rights of contractors. The current rule language potentially allows for contractor-funded technical data to be "swept in" to the Government with unlimited rights. The rules should be revised to make clear that only data created as a direct charge against a Government contract, and for which full funding has been paid by the Government, will be taken by the Government with unlimited rights (with the noncontroversial exceptions for form, fit, and function data, etc.).

Revision 2. Contractor nondelivery of sensitive data. At a minimum, in consonance with the discussion in Recommendation 4 above (and even without adoption of Recommendation 2), the DFARS should be revised to permit delivery of only form, fit, and function data when the data are created at private expense. Contract clause alternates should be created, as in the FAR, for delivery of only form, fit, and function data under these circumstances (see the further discussion below). Clauses and policy should also be developed to use escrow and contractor storing of data with DoD march-in rights upon the happening of appropriate events (or upon the order of, say, the Secretary of Defense or another high-level DoD official).

Recommendation 7: DoD should revise MIL-T-31000 technical data delivery requirements for clarity.

The current version of this specification is not clear about certain points that are very critical to industry. Although the DID for product drawings contained in the specification indicates that only form, fit, and function data need be delivered for

limited rights items, the language is not precise, and it is not clear whether this is mandatory for the Government. The DID states

> *Limited rights-in-data items.* Product Drawings for items for which the government does not have unlimited rights in data shall specify the form, fit and function requirements of the item and conform to 200.4 of DoD-STD-100. (par. 10.8)

What about items for which DoD has GPLR? This specification language would seem to say that DoD could only take form, fit, and function data for these items. Yet that would impair procurement from alternative sources, which is the whole purpose of GPLR. One explanation would be that the writers believed, as used to be the case, that there were only two categories of rights in technical data – limited and unlimited. This should be corrected to reflect the latest regulation creating GPLR.

Furthermore, it is not clear whether the DID and its exception for limited rights data are mandatory. The DID is found in Appendix A of MIL-T-31000 and is referenced in Par. 6.3 of the specification. That paragraph states:

> *Data requirements.* The following Data Item Descriptions (DIDs) must be listed, as applicable, on the Contract Data Requirements List (DD Form 1423) when this specification is applied on a contract. . . .

The DID for product drawings is then listed with others. But section 6 in its entirety is introduced with this note: "This section contains information of a general or explanatory nature that may be helpful, but is not mandatory."

We recommend that this ambiguity – with regard to whether the DID, with its call for delivery only of form, fit, and function data, is mandatory or not – be clarified and that the DID with its exception for limited rights data be incorporated in all contracts. Also, a clause alternate supporting the exception (noted above) should be included in the DFARS.

REFERENCES

[1] James W. McKie, *Proprietary Rights and Competition in Procurement*, Santa Monica, CA: The RAND Corporation, June 1966.

[2] Donna C. Maizel, "Trade Secrets and Technical Data Rights in Government Contracts," *Military Law Review*, Vol. 114, 1986.

[3] Robert A. Brunette, "U.S. Congress Requires Limitations on Competition for Innovative Defense Contracts and Subcontractors," *National Contract Management Journal*, Vol. 23, No. 1, Summer 1989.

[4] Department of Defense, Report to the Secretary of Defense by the Under Secretary of Defense (Acquisition), *Bolstering Defense Industrial Competitiveness: Preserving Our Heritage, Securing Our Future*, Washington, DC: U.S. Government Printing Office, July 1988.

[5] LMI Report PL106R1, *A Profile of Defense Manufacturing Costs and Enabling Technologies*, Eric L. Gentsch and John W. McInnis, January 1992.

[6] John J. Keller, "R&D Hardball: Defying Boss's Orders Pays Off for Physicist and His Firm, AT&T," *The Wall Street Journal*, 25 June 1991.

[7] Paul Mann, "Packard Proposes Company Performance as Standard for Weapon Contract Awards," *Aviation Week & Space Technology*, Vol. 129, No. 6, 8 August 1988.

[8] U.S. Congress, Office of Technology Assessment, *Redesigning Defense: Planning the Transition to the Future U.S. Defense Industrial Base*, OTA-ISC-500, Washington, DC: U.S. Government Printing Office, July 1991.

[9] Ralph C. Nash, Jr., "Government Rights in Technical Data: Recent Court Decisions," *The Nash & Cibinic Report*, Vol. 3, No. 12, December 1989. Also, "Government Rights to Subcontractor Technical Data: A Flowdown Problem," *The Nash & Cibinic Report*, Vol. 2, No. 10, October 1988.

[10] "Federal Appeals Court Restricts DoD Access to Trade Secrets," *Aerospace Daily*, Vol. 151, No. 42, 31 August 1989.

[11] "Wagner Wants Proprietary Rights Challenged," *Defense Daily*, Vol. 156, No. 21, 2 February 1988.

[12] Robert Holzer, "Data Rights Policy Places Seawolf in Hot Water," *Defense News*, 18 December 1989.

[13] Steve Ryan, "Data Rights Controversies Swirl Around Navy Contracts," *Navy News and Undersea Technology*, Vol. 6, No. 47, 4 December 1989.

[14] "Army Rewrites LHX DEM/VAL Contract After Protest," *Helicopter News*, Vol. 14, No. 23, 18 November 1988.

[15] Arthur J. Alexander, Paul T. Hill, and Susan J. Bodilly, *The Defense Department's Support of Industry's Independent Research and Development (IR&D): Analyses and Evaluation*, Santa Monica, CA: The RAND Corporation, April 1989.

[16] U.S. General Accounting Office, National Security and International Affairs Division, *DoD Efforts Relating to Nondevelopmental Items*, GAO/NSIAD-89-51, Washington, DC: U.S. General Accounting Office, February 1989.

[17] David V. Lamm, *An Analysis of Reasons Companies Refuse to Participate in Defense Business*, NPS Report 54-87-003, Monterey, CA: Naval Postgraduate School, March 1987.

[18] David V. Lamm, "Why Firms Refuse DoD Business: An Analysis of Rationale," *National Contract Management Journal*, Vol. 21, No. 2, Winter 1988.

[19] Jon Arthur Schauber, *An Analysis of the Reasons Why Nonferrous Foundry Subcontractors Refuse to Participate in DoD Business*, Monterey, CA: Naval Postgraduate School, June 1988.

[20] Department of Defense, *Defense Procurement Industrial Base Study: Why Firms Are Leaving the Defense Market*, Ft. Belvoir, VA: Defense Systems Management College, 5 December 1990.

[21] Lt. Col. David Scribetta, telephone interview, 17 April 1991.

[22] Curtis R. Cook, "Spare Parts Procurement Within the Department of Defense: Separating Fact from Fiction," *National Contract Management Journal*, Vol. 23, No. 2, 1990.

[23] Richard R. Kaeser and Jonthan P. Blucher, "Technical Data Rights: How They Work – Why They Won't," *The Air Force Law Review*, Washington, DC: U.S. Government Printing Office, 1988.

[24] *Establishing Competitive Production Sources: A Handbook for Program Managers*, prepared by L. A. Kratz, J. W. Drinnon, and J. R. Hiller for the Defense Systems Management College, ANADAC Inc., August 1984.

[25] Stephen C. Miller, *A Study of the Effect of Dual Sourcing on Operation and Support*, AFIT/GCM/LSQ/88S-9, Wright-Patterson Air Force Base, OH: Air Force Institute of Technology, September 1988.

[26] Dan C. Boger, Willis R. Greer, Jr., and Shu S. Liao, *Competitive Weapon Systems Acquisition: Myths and Facts*, Monterey, CA: Naval Postgraduate School, March 1989.

[27] Donald L. Pilling, *Competition in Defense Procurement*, Washington, DC: The Brookings Institution, 1989.

[28] Karen W. Tyson, J. Richard Nelson, Neang I. Om, and Paul R. Palmer, *Acquiring Major Systems: Cost and Schedule Trends and Acquisition Initiative Effectiveness*, Alexandria, VA: Institute for Defense Analyses, March 1989.

[29] Kemal Guler and Charles R. Plott, *Private R&D and Second Sourcing in Procurement: An Experimental Study*, Social Science Working Paper 684, Pasadena, CA: California Institute of Technology, October 1988.

[30] U.S. General Accounting Office, *Cost Effectiveness of Dual Sourcing for Production Price Competition Is Uncertain*, GAO/NSIAD-84-111, Washington, DC: U.S. General Accounting Office, 31 August 1984.

[31] Department of Defense, *Report on the Audit of the Spare Parts Breakout Program*, Report No. 90-056, Arlington, VA: Department of Defense Inspector General, 5 April 1990.

[32] James Kitfield, "Cheaper Spares, But at What Price?", *Military Logistics Forum*, June 1986.

APPENDIX A

EVOLUTION OF CURRENT TECHNICAL DATA POLICIES AND CONTROVERSIES

WORLD WAR II AND AFTERMATH

In its entire history prior to World War II, the United States had never had a large standing peacetime Army and Navy. Neither did it have a large industry dedicated to the support of the professional Army and Navy. The Military Services either bought commercial equipment for their needs or designed military items themselves (in house) and then either built the item in Government arsenals or merely contracted for their manufacture. Conflicts and issues about rights in technical data did not arise [A-1].

During World War II, and slightly before, that situation began to change. Private firms commenced large-scale participation in the design and development of weapon systems. These private firms began to claim "proprietary" interests in some designs, components, and manufacturing processes incorporated into the weapon systems they helped build.

After the war, the United States accepted a vast global responsibility and the requirement for a large committed force to go with it. With that radical historical change, a defense industry began to emerge consisting of corporations selling primarily or exclusively to the military and participating directly and intimately in the entire design, development, and production processes.

Yet even with this advent of private company proprietary claims, there were no serious conflicts over rights in technical data in the early years following World War II. That was principally because the Military Services did not make any use of their contractors' technical data that could threaten the contractors' vital economic interests, such as providing the contractor-developed data to another manufacturer. The Military Services, combined into the Department of Defense in 1947, simply bought all their equipment from the original supplier and allowed prime contractors to do the same with their own vendors. In addition, at least through the end of the Korean War, defense contractors were working to capacity and thus were not

seriously concerned about alternative sources of supply for their equipment. There was enough business to go around [A-1].

In 1948, Congress passed the Armed Services Procurement Act, which established the basic statutory framework of rules for procurement by the Department of Defense. Soon after, the Department implemented the Act with its own regulation, the Armed Services Procurement Regulation (ASPR). Early versions of this regulation contained no separate contract clauses for rights in technical data other than data protected by patent or copyright. The early DoD Patent Rights clause, ASPR 9-107.1, did contain a subparagraph (d) dealing with rights in technical data. This provision was included in all contracts for experimental, developmental, or research work [A-2].

POST-KOREAN WAR

After the Korean War, the situation once again changed dramatically. Weapon systems escalated in cost and complexity. As a direct consequence, the number of systems and their variety were drastically reduced. Congressional critics and others began to complain about DoD sole-source procurements, believing these were the cause of excessive costs, and about the lack of opportunity for some firms to participate in the defense market. This led to an increased DoD focus on controlling costs as well as "breaking out" components and subsystems of weapons, such as engines, for procurement competitions separate from the main system. The purpose of this breakout was to give more suppliers a chance to share in the defense production business and to eliminate the mark-up that prime contractors tacked on to the price of components supplied to them by subcontractors.

The new emphasis on competition also led DoD to adopt the practice of competitive reprocurement of equipment. As contrasted with breakout of components for competitions for the initial production, in competitive reprocurement DoD took the technical data developed by an initial contractor and distributed the data to other potential bidders for subsequent production, thus breaking down the sole-source position of the original manufacturer. DoD was able to do this because the original manufacturers had been delivering the data as required under their contracts. Although most of these contracts under which the data were delivered were for research and development (and thus were being directly funded by DoD), the contractors regarded much of the data as proprietary. At the same time, these

defense suppliers were experiencing the dramatic decline in production and rapid increase in their own unused capacity as the nation demobilized. They began to be more protective of their defense business [A-1].

In January 1955, the ASPR patent clause paragraph (d) was made a separate contract clause, Technical Data in Research and Development Contracts, ASPR 9-112 [A-2]. The clause, which was required in all contracts for "experimental, development or research work," gave the Government all rights to reproduce, use, and disclose data for "governmental purposes (including the right to give to foreign governments for their use as the national interest of the United States may demand)." The clause made no provision for protecting a contractor's proprietary data if the data were required to be delivered under the contract. The only explicit limitation imposed on DoD was the "governmental purposes" requirement. Contractors at first thought they were protected by that language, because they did not think competitive reprocurement could be regarded as a governmental purpose. DoD, however, tended to regard the language as authorizing virtually any use of the data by DoD. The courts did not fully support DoD's interpretation and found,[1] for example, that DoD's use of drawings to manufacture guns for supply to other countries was a compensable breach of contract [A-2].

Industry protested vehemently against this clause and the loss of what they regarded as their proprietary technical data under it. In response to those objections, DoD revised the regulation in 1957 and again in 1958 [A-1, A-3].

THE 1958 RULE

In the 1958 revisions [ASPR 9.202-1(a)], DoD stated its intention

> . . . to encourage inventiveness and to provide incentive there for it by honoring the "proprietary data" resulting from private developments and hence to limit demands for data to that which is essential for Government purposes. . . . Generally it should not be necessary to obtain "proprietary data" to satisfy Government requirements . . . [Contractors] should not request unlimited rights in "proprietary data" [from subcontractors] where such rights are not required by the Government under the prime contract. [A-1, A-3]

[1] Aktiebolaget Bofors v. United States, 139 Ct. Cl. 642, 153 F. Supp. 397 (1957).

"Proprietary data" was defined [ASPR 9.201(b)] as

> ...data providing information concerning the details of a contractor's secrets of manufacture, such as may be contained in but not limited to its manufacturing methods or processes, treatment and chemical composition of materials, plant layout and tooling, to the extent that such information is not disclosed by inspection or analysis of the product itself and to the extent that the contractor has protected such information from unrestricted use by others. [A-3]

This definition was based on the common law concept of "trade secrets." That concept allowed a person to protect a secret and to prevent unauthorized release of that secret when the creator disclosed it in confidence to others, such as under a license arrangement. Under appropriate circumstances, the courts would enforce the creator's right to keep the information "secret" and would penalize violators of the confidence. Unlike a patent, a trade secret was not a property right. It was a protected monopoly only as long as the originator diligently maintained the secret.

Many contractors had a much broader view of "proprietary" than the Government concept expressed in this definition. They believed that all suppliers' designs should be protected *in their entirety*, not just "secrets of manufacture." They argued that in the commercial world, ethical competitors did not pirate the designs of others. They might borrow design *concepts* or imitate others' improvements, but they would create their own designs to meet performance requirements and not make identical copies of another company's hardware. The Government, they argued, should similarly recognize the entire product as proprietary and should never get other manufacturers to reproduce parts (other than perhaps standard, simple items like nuts and bolts) designed by another company. In other words, their concept of proprietary was based more on an ethical idea than on trade secret law [A-1].

The 1958 revisions provided separate rules for supply contracts and research and development contracts. In supply contracts, contracting officers were prohibited from requesting proprietary data when the contract was awarded through the sealed bidding process or when the contract was for a standard commercial item. In all other supply contracts, proprietary data could be requested only when a clear Government need for the data had been established and specifically negotiated.

In contracts having experimental, developmental, or research work as one of their principal purposes and calling for models of equipment or practical processes, the contractors were required to furnish for the price of the work "all data resulting

directly from performance of the contract, regardless of whether it was 'proprietary data.'" In addition, the contractor was required to furnish all data necessary "to enable reproduction or, where appropriate, manufacture of the equipment or performance of the process." Two exceptions [ASPR 9.202-1(c)] were provided:

- Standard commercial items that were incorporated as component parts in or were to be used with the product or process being developed. The contractor had to identify source and characteristics sufficient to enable the Government to practice the process or procure the part or an adequate substitute.

- Other items, including minor modifications thereof, that were developed at private expense and previously offered for sale and that were incorporated as component parts in or to be used with the product or process being developed. For such items, proprietary data did not have to be provided, but the contractor had to identify any items and data that were both proprietary and necessary to manufacture the item or perform the process. For other previously developed proprietary data necessary for manufacture of the item or practice of the process, contracting officers could negotiate a suitable price [A-3].

A key proviso was added to the 1958 basic data clause for production contracts, stating that the contractor could withhold any proprietary data that was not specifically identified by the contract Schedule as required. So, for example, in a part drawing the contractor could eliminate any information relating to chemical processes, tooling, finishing, temperature tolerances, lamination, milling, and inspection techniques.

This single proviso opened the door to vast unexpected consequences. Contractors often withheld all data even arguably tinged with a proprietary claim. Some contractors would substitute their own specifications of materials and processes for more standard ones, then claim proprietary rights and withhold the data. During development, contractors often would change a design in which DoD had unlimited rights and substitute new proprietary data for the original data. And vendors would refuse to deliver data in any form to prime contractors because of fear that their trade secrets would be compromised. Since the Government did not have the data in its physical possession, it was in a weakened bargaining position to challenge the proprietary claims. And the volume of data received made it impossible to challenge all but a fraction of contractors' submissions [A-1].

The result was a disaster for DoD. Both the quality and completeness of Government-held data deteriorated to the point that the data were often worthless for any purpose, not just competitive reprocurement. Maintenance, repair, overhaul, stockpiling, and supply all suffered from lack of necessary technical information [A-1].

THE 1964 RULES

The failure of the 1958 rules led to another fundamental policy shift, in 1964. The resulting policy is basically the one in effect today. It substituted a new data rights test for the old proprietary standard based on trade secret concepts. The new test was based on the source of funding.

Under the new rules, technical data pertaining to items, components, or processes developed at private expense would be acquired by DoD with "limited rights." By limited rights DoD meant that the data could be used only within the Government. It could not be used for manufacture or procurement or otherwise released outside the Government. Technical data developed with any Government funding would be taken by the Government with "unlimited rights," meaning that the Government could do anything with it. Also, technical data resulting directly from an R&D contract or subcontract would be acquired by the Government with unlimited rights, regardless of source of funding. "Form, fit, and function data" (product descriptions sufficient to identify physically and functionally interchangeable products) would also be acquired with unlimited rights, no matter who funded development of the item or data.

The rules provided that the Government and contractor could negotiate in advance to determine which category of rights specific data would receive. Contractors were required to notify the Government in advance if they intended to use in an R&D contract any component or process in which the Government would have only limited rights. And subcontractors could deliver their limited rights data directly to the Government, rather than through the prime contractor [A-1].

THE SPARE PARTS BREAKOUT PROGRAM

At about the time when DoD shifted to its new technical data rules, it also initiated a new program to introduce more competition in the procurement of spare parts, with the aim of reducing the prices on those parts. The new program, called

the "High-Dollar Breakout Program," instituted a process of screening parts for possible competitive procurement as soon as possible after a weapon system was acquired, usually before or during "initial provisioning." Initial provisioning is the practice of providing an initial volume of spare parts with a new system at the time it is first introduced into the field.

The screening took place in two steps: First, the prime contractor identified whether a part was suitable for competitive procurement or could be purchased from designated subcontractors or must be procured only from the prime contractor itself. Then the DoD procuring office would conduct its own screening of the prime contractor's effort for all items having an expected high annual procurement value. The procuring office also sampled other parts codings to check that the prime contractor was not unfairly restricting purchases to itself.

During the screening, parts were evaluated to determine whether they were "critical." Critical meant that failure of the part could cause serious failure of the parent equipment or system. Criticality could include such constraints as the need for master tooling, interface compatibility, and special tests and inspection procedures. These constraints usually dictated that the part be bought from the original manufacturer, and so no manufacturing data for procurement was needed by the Government. This procedure reduced conflict between DoD and the contractor over data rights [A-1].

THE 1980s

As the Reagan Administration began to invest heavily in a rapid defense buildup, critics of the buildup itself and of the manner in which it was being conducted began surfacing one "horror story" after another about alleged grossly overpriced hammers, diodes, Allen wrenches, coffee pots, toilet seat covers, and other spare parts and common items. Congress and public were incensed. The problem once again, according to congressional critics, was that DoD was buying too much from sole-source suppliers. The solution, they were certain, was more competition at every stage and phase of defense procurement. They were also concerned that one of the main reasons that DoD was not competing its spare parts acquisitions more was that it was not receiving the necessary rights in technical data. In addition, small businesses repeatedly testified that they were being cut out of defense parts

procurements because DoD lacked the technical data needed to manufacture the parts [A-3].

In response to this situation, Congress passed two key statutes in 1984. The first of these was the Competition in Contracting Act of 1984 (CICA) [Public Law (P.L.) 98-369]. The CICA mandated "full and open competition" in all Federal procurements, with seven narrow exceptions permitted. Approval to use the exceptions was made difficult and had to be justified by the agency in writing.

The Defense Procurement Reform Act of 1984 (P.L. 98-525), passed 3 months later, had the specific intent of dealing with alleged excessive prices for DoD's replenishment (spare) parts. As with CICA, the Act emphasized competition, but it further focused on rights in technical data. The Reform Act required that in both development and production contract solicitations for major systems DoD consider requiring offerors to give DoD the rights necessary to reprocure spare parts from other sources [A-4].

The Reform Act was later amended, after industry objections, and now *prohibits* DoD from requiring contractors, as a condition of doing business with DoD, to relinquish their rights in technical data that would enable DoD to competitively reprocure the item. The Reform Act permits two exceptions: (1) When DoD determines that the original supplier will be unable to satisfy program schedule or delivery requirements or (2) when the original supplier does not satisfy DoD that it can meet mobilization requirements.

The Reform Act also established an elaborate set of procedures for challenging and validating contractor claims in technical data. Other changes to the law now require negotiations between the contractor and DoD to determine data rights when both parties contributed funds in the development of an item or process.

Having dealt with the spare parts issue, Congress next focused its attention on the major weapon systems themselves. In 1985, it passed P.L. 99-145, requiring that all defense major systems acquisitions provide for competitive alternative sources for the system and each major subsystem from the beginning of full-scale development *through the end of production.* Exceptions were provided if the Secretary of Defense determined, for example, that alternative sourcing would produce unacceptable costs or delays or would be adverse to national security interests. But if an exception was exercised for a particular program, the Secretary was required to report this, with

detailed justifications, to Congress. In the FY91 DoD Authorization Act, this section of the U.S. Code (10 U.S.C. 2438, formerly 2305a) was amended to eliminate the presumption in favor of alternative sourcing for major systems and the onerous reporting requirements. The law now requires only that major system acquisition strategies include the *option* of alternative sourcing, if that would reduce risk or cost or result in improved design without undue delay or adverse national security consequences (P.L. 101-510, Section 805).

The Defense Department responded to these and other statutory requirements with a series of regulation changes. The final such change was published as an interim rule in October 1988 and remains in effect today.

REFERENCES

[A-1] James W. McKie, *Proprietary Rights and Competition in Procurement*, Santa Monica, CA: The RAND Corporation, June 1966.

[A-2] Ralph C. Nash, Jr. and Leonard Rawicz, *Patents and Technical Data*, Washington, DC: The George Washington University, Government Contracts Program, 1983.

[A-3] Donna C. Maizel, "Trade Secrets and Technical Data Rights in Government Contracts," *Military Law Review*, Vol. 114, 1986.

[A-4] Robert A. Brunette, "U.S. Congress Requires Limitations on Competition for Innovative Defense Contracts and Subcontractors," *National Contract Management Journal*, Vol. 23, No. 1, Summer 1989.

APPENDIX B

DEPARTMENT OF DEFENSE ORDERING AND MANAGEMENT OF TECHNICAL DATA

Ordering technical data from contractors is very expensive. And as we have seen, it can also produce intense conflict between DoD and its contractors and subcontractors. We have noted that it is DoD's stated policy that the agency acquire only its minimum essential needs in technical data. Defense FAR Supplement (DFARS) 227.402-71 states: "The Department of Defense shall obtain only the minimum essential technical data and data rights." DoD Instruction (DoDI) 5000.2, Part 9, Section B, "Technical Data Management," paragraph 3(a)(2) states: "Only the minimum data needed to permit cost-effective support of research, development, production, cataloging, provisioning, training, operation, maintenance, and related logistics functions over the life cycle of the item will be acquired." But what are the "minimum essential needs" for a particular weapon system or product? How are these minimum essential needs determined and how do they get included in the contract between DoD and the contractor?

The process begins as the contract solicitation is being developed within the agency. At that time, the integrated logistics support (ILS) manager assigned to the particular acquisition circulates a procurement package describing the statement of work and other relevant aspects of the procurement to all of the logistics element managers (for example, those responsible for maintenance engineering, technical manuals, and initial parts provisioning), who will determine what technical data will be needed for that particular product in its useful life. The logistics element managers consider all the potential needs for data from development and production of the weapon system through operational support. They do not normally consider rights-in-data issues at this time. This process of circulating the acquisition characteristics to the logistics element managers for their input to data requirements is known as the "data call."

The ILS manager delivers the results of the data call for the particular acquisition to the technical data manager. These data requirements are then supposed to go through a process of review to see whether they are excessive. The

technical data manager is to give the requirements a first check. Furthermore, DoDI 5000.2 requires that a data requirements review board be established to review all data call recommendations and advise the program manager. When the acquisition has a potential cost of $5 million or more, the board must be convened before the solicitation is issued [DoDI 5000.2, Part 9, Section B, paragraph 3(a)(1)].

Data requirements that survive the review process are listed on a special form, the Contract Data Requirements List (CDRL), DD Form 1423. This list becomes an element of the contract. Only technical data requirements identified on the CDRL must be delivered by the contractor as part of contract performance. The CDRL relates each data deliverable to a task in the statement of work and to a specific data item description that describes the content of the deliverable and specifies where and when delivery is to be made.

During the solicitation phase for the contract, CDRL prices are negotiated with offerors, with each CDRL item usually priced separately. If the prices quoted for a particular data deliverable item are extremely high and offerors will not significantly change their prices during negotiation, the contracting officer may decide to drop the data requirement from the contract or to negotiate an alternative. Furthermore, contractors may propose to delete certain data requirements as unnecessary or too expensive. They may suggest tailoring the requirements, propose alternatives, or take exception to the requirements in their proposal.

Does this process produce contracts in which only the Government's minimum essential needs are acquired? There is a general belief that DoD acquires a large amount of data that it does not use or that is much too expensive for the benefit received [B-1, B-2]. The causes of this are many, as discussed below.

DATA ORDERING

Data requirements are specified at a stage in the contracting process when the uncertainties about the life of the item being acquired are great. Military weapon systems tend to have very long life cycles, much in excess of commercial systems. Since the long-term future of the system is uncertain, there is a natural tendency on the part of the logistics experts to "play it safe" and order the maximum amount of data potentially needed [B-1]. Unfortunately, technical data generally must be ordered and created during development and production if they are to be obtained at all. Once the design and production teams have been disbanded, it can be difficult if

not impossible to create or correct technical data after the fact. This, too, leads logisticians to order more data – as insurance against unforeseen contingencies – than they might otherwise. Ordering only technical data for which a clearly established need and benefit exists would often increase the risk that the item would become unsupportable prematurely in its life cycle.

The logisticians who order the data normally do not know the cost of the data. Their orders are based primarily on their assessments of potential need for technical data rather than on a calculation of benefits compared to costs or "best value" considerations. Because cost is not a factor in determining initial data requirements, the bias is toward ordering more, not less.

Program managers are officially rated on their ability to keep to cost and schedule goals. This can result in either too much or too little technical data being acquired. If schedule is the primary consideration, then too much data may be ordered because the necessary time to review data requirements may be cut. Or, on the other hand, schedule considerations may result in too little data being ordered if schedule constraints cause the Government to relieve contractors of data delivery requirements or if sanctions necessary to assure delivery of acceptable data are waived because they might cause the overall schedule to slip. If program cost constraint is the primary goal, then data deliverables may be cut with minimal regard for the long-term impact on logistics support.

DATA REQUIREMENTS REVIEW

During the data call for a new weapon system, as many as 13 separate disciplines can submit data requirements for incorporation in the CDRL. It is nearly impossible for the data manager to be conversant enough in all those disciplines and in the particular acquisition item and strategy to challenge those requirements confidently. Furthermore, data managers are often responsible for many different contracts or perhaps for hundreds of deliverables on a single, large contract. Under such conditions, the manager is forced to be very selective in reviewing proposed contract data requirements.

Requirements reviews often consist of a cursory comparison of deliverables to the acquisition schedule and perhaps some review of the largest deliverable requirements, to identify major discrepancies. There is usually not enough time to conduct detailed analysis of deliverables and look for other alternatives. Managers

rely on formulas and precedents to a large degree in processing contract data requirements. Even when discrepancies or better alternatives are discovered, the data manager must go back to the original proponent of the data requirement to coordinate a change. Rarely can a data manager act independently of the originator of the data requirement.

CONTRACTOR PROPOSALS

Program managers often rely on contractors to challenge data requirements as excessive and to propose where data requirements might be deleted, tailored, or replaced by a substitute approach. But contractors are often concerned that too much questioning of DoD's data requirements or proposing of novel approaches to those requirements might result in their being found nonresponsive to the solicitation. Contractors are also under time pressure to submit their proposals and thus do not always have time to analyze requirements and price alternatives. And in many cases, especially in cost-reimbursement contracts, they may not have a strong incentive to propose reductions in the cost.

DEFERRED ORDERING AND DELIVERY

As noted, one of the main causes for excessive data ordering is the fact that data requirements are determined at a very early stage of the acquisition, usually during solicitation of the original development contract. Since the future uses of the item being developed are very uncertain at that stage, there is a clear tendency to order data for all conceivable contingencies. Recognizing this, DoD encourages its buyers to use deferred ordering or delivery of the technical data as a way of controlling costs. These techniques allow the contractor to finalize the design before the data are submitted to the Government. Thus the Government does not pay repeatedly for many revisions of data while the design of the weapon system is undergoing significant change.

Deferred delivery lets the contracting officer postpone the actual date of delivery until the design is finalized. Delivery can be deferred up to 2 years after Government acceptance of the item under the contract. This procedure reduces both storage costs and the costs of buying data made obsolete by hardware changes.

Deferred ordering permits the contracting officer to wait to order data until a firm requirement is established. Under the relevant DFARS contract clause, the

contracting officer may delay ordering any technical data produced as part of the performance of the contract for up to 3 years after contract termination or acceptance of all items under the contract. If data are ordered, the Government pays the contractor the cost of converting them into the prescribed form, reproduction, and delivery but not for creating the data in the first place, since that has already been paid for under the contract. Of course, this cost of conversion is minimal compared to the already-sunk cost of creating the data. DoD managers may thus conclude that it is worth the marginal additional expense to have the data in hand.

A major problem in deferred ordering is the potential difficulty of enforcement, since the contractor has already been paid for the major work on the contract. The amount of additional compensation the contractor can receive for performing this requirement is minimal. About all the Government can do is threaten the contractor with taking the performance failure into account in future source selection evaluations.

Furthermore, the clauses do not save the major costs of producing the data in the first place. Under the contract, the contractor is still required to produce the data, and the Government is still required to pay for that effort.

DATA STORAGE AND CUSTODY

Generally, technical data delivered by the contractor and accepted by the Government are stored in DoD data repositories, along with similar data for other weapon systems and equipment. Most data are stored in paper or microform media. Physical access to the data in the repository is limited to repository employees and other DoD employees who are known to have direct job-related need for access to technical data. Procedures to control access to the repository include sign-in/sign-out procedures and mandatory escort of visitors.

Technical data within repositories are released to authorized requesters only. A combination of directives, local guidelines, and repository manager oversight determines who will be granted the privilege of access to technical data. Access authorization is based on the employment status of the requester (Government or non-Government), the rights restrictions of the requested data [unlimited, limited, or Government purpose license rights (GPLR)], whether the data are to be released outside the Government, and the intended use of the data by the requester.

As a rule, repositories will release any available technical data to Government requesters whose job requires access to technical data on a routine basis or who have justified their need for technical data on a case-by-case basis. The technical data manager must approve unusual requests, in accordance with established guidelines. Government personnel receiving limited rights or GPLR data are under the same obligation as the repository to ensure that the data are used for internal Government purposes only.

While release of technical data to DoD employees focuses on whether or not the requester has the necessary access authority, release of technical data to requesters from outside the Government focuses on the rights status of the data. Most requests for external release of technical data are from potential offerors who wish to compete for DoD procurement of components and parts. In deciding whether to break out an item for competitive procurement, DoD will determine whether any part of the technical data package for the item contains limited rights data. If it does, then competitive procurement is abandoned and the equipment will normally be purchased from the original equipment manufacturer (of the larger item containing a component) or, preferably, from the actual manufacturer(s) of the component. If the data package contains GPLR data but no limited rights data, DoD will competitively procure the part, component, or item. All potential bidders will be required to sign applicable licensing or nondisclosure agreements prior to receipt of the technical data necessary to bid or perform the work. Only if a complete data package contains entirely unlimited rights data will DoD distribute the package widely for unrestricted competitive procurement.

The Defense Department employs the following safeguards, among others, to protect data in which it has less than unlimited rights:

- *Supervisory oversight.* Supervisors certify the needs of their subordinates to have access to technical data and share responsibility for proper use of the data.

- *Technical data manager oversight.* The technical data manager has primary responsibility for ensuring proper safeguarding of technical data stored in repositories under his control, including control of distribution. He is guided by DoD, Military Service, and field activity directives and Federal law (such as the Freedom of Information Act). Technical data managers often personally decide on unusual data release requests or make recommendations to the local facility commander for decision.

- *Physical restrictions.* Data are stored in data repositories that are restricted-access areas. All people entering the repository must identify themselves, be on official business, sign in and out, and be properly escorted.

- *Data indexing.* In addition to markings on individual drawings, the rights status of technical data is included in electronic drawing indexes, and software is programmed to identify and preclude automatic distribution of data packages containing limited rights or GPLR data.

- *Procurement method coding.* When a new item enters the supply system, it is reviewed for the appropriate procurement method. If limited rights or GPLR data are present in the data package, the item is coded for procurement other than by means of full and open competition.

- *Engineering review.* Engineers review available data prior to solicitation to determine whether the item is technically suitable for competitive procurement [that is, whether the technical data package (TDP) is adequate for a competent manufacturer to make the item to specification from the available technical data]. Rights to the data package are reviewed at the same time to determine whether DoD's rights to the TDP prohibit distribution to potential bidders or require recipients to sign nondisclosure or license agreements.

As described here, DoD checks the rights status of newly delivered data twice (procurement method coding and data indexing), checks on the authority of data requesters for each release of technical data, and checks the rights status of the TDP at least three times before releasing solicitations (at the repository, during the engineering review, and at the procurement office).

Yet, in spite of all these controls, DoD contractors widely believe that their sensitive data in DoD repositories are not safe from unauthorized disclosure or "leakage" to their potential competitors. This is not surprising, since these same contractors often have the same sense of insecurity even with their own employees and often employ extensive security controls. This lack of contractor confidence in DoD's ability to keep sensitive data safe is intensified when it comes to the prospect of DoD protection of data in a Computer-aided Acquisition and Logistic Support environment.

REFERENCES

[B-1] Ralph C. Nash, Jr. and Leonard Rawicz, *Patents and Technical Data*, Washington, DC: The George Washington University, Government Contracts Program, 1983.

[B-2] Lt. Gen. James Stansberry (USAF, Ret.), "Defense Procurement Process," testimony given in a hearing before the Subcommittee on Defense Acquisition Policy of the Committee on Armed Services, United States Senate, Part 4, 20 February 1985, Washington, DC: U.S. Government Printing Office, 1985.

APPENDIX C

COMMERCIAL PRACTICE AND TECHNICAL DATA

LICENSING

One strategy used in today's high-technology markets is to license less sensitive (usually older) technologies to other firms. Such licenses produce what can be an important income stream from royalties or else a lump sum paid by the licensee to the source company. Companies may choose to transfer a product technology to another firm under a licensing agreement for several reasons. They may want to recoup their R&D investment sooner to pursue a promising new R&D venture (in other words, the license becomes a source of capital for new product development). The transfer may occur because of limited ability to expand to meet demand or when the technology is to be a component of a larger item that the innovator cannot or will not make. Or, finally, it may occur when the licensee can produce the product at a lower price, even with royalty payments to the source firm (see discussion below).

A high-technology company will almost never license its newest product technologies to a potential competitor in its own market, because as a result of losing its monopoly on the product, the company cannot charge the premium prices [C-1] necessary to recover the costs of past development and pay into future development. This point is critical. Companies will invest their resources where they will earn the best return, other things being equal. And it would be a highly unusual situation in which income from a license could make up for the income lost from losing the monopoly position in the market. There is also the increased risk that the licensee may improperly release or transfer the technology further, with the result that even more market revenues would be lost to the source firm. Of course, if a company were willing to pay enough to compensate the source for the full economic value of the product and its underlying technology, a bargain could be struck.

One exception to the rule against licensing one's newest technologies occurs when the recipient firm can produce the product more profitably than the source firm (e.g., when it has lower wage rates). Then it may make sense for the source to license the recipient, charge a premium fee, and abstain from production itself. Since the

recipient firm's lower costs allow it to bring it the monopoly profits even with the high royalty, both companies benefit [C-1].

Another possible exception may apply in the case of a very large potential customer that insists on the establishment of a second source for the product as a condition for buying it from the innovator. The innovator firm must then weigh the loss of premium revenues from its monopoly position against the anticipated profits from sales to the large customer. The decision will turn very much on the size of the sales to the large customer and the terms the customer has offered, as well as conditions in the rest of the market [C-1]. Again, the matter will be decided primarily on a calculation (to the extent possible) of where the company's critical resources will earn the best return. As we noted, if the price is right, the source will sell. This situation, of course, assumes that the large customer has access to at least some reasonable alternatives that can meet its needs or that it can do without the product altogether if necessary (in such a case, the seller probably cannot command a full monopoly premium anyway). Otherwise, the seller can simply tell the customer to take it or leave it.

Generally, then, companies will license only their older technologies as they aggressively push the state of the art in their product lines. Staying at the leading edge of the market is also a firm's protection against license abuse by licensees, since the licensee will want to retain good relationships with the source firm to keep up a steady stream of the older technologies released from the source.

PROTECTING TECHNICAL DATA – LEGAL CONCEPTS

Companies generally try to protect their most valuable technical information either by acquiring a patent or by maintaining the data as a trade secret. A patent is a right granted to an inventor by the U.S. Government after an examination of the inventor's application to determine that the "invention" meets statutory requirements. Patents can be issued for any "new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof."[1] If the invention meets a host of criteria, it receives a patent for 17 years, giving the recipient the "right to exclude others from making, using, or selling the invention throughout the United States . . . ."[2] The inventor is given a monopoly to

[1] 35 U.S.C. Section 101.

[2] 35 U.S.C. Section 154.

"practice the invention" on the condition that the invention be openly published so others may learn and benefit from the new knowledge incorporated in it. During the 17-year period, anyone wishing to use the patented item or process must attempt to get an agreement (usually a license with a royalty fee) from the inventor.

The trade secret is a concept developed under common law that gives legal protection to certain business information under certain circumstances. Although an exact definition of a trade secret "is not possible," according to the legal authority titled *Restatement of Torts*, an accepted definition is

> . . . any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it. It may be a formula for a chemical compound, a process of manufacturing, treating or preserving materials, a pattern for a machine or other device, or a list of customers. [C-2]

Further, the *Restatement* says that

> A trade secret is a process or device for continuous use in the operation of the business. Generally it relates to the production of goods, as, for example, a machine or formula for the production of an article. It may, however, relate to the sale of goods or to other operations in the business, such as a code for determining discounts, rebates or other concessions in a price list or catalogue, or a list of specialized customers, or a method of bookkeeping or other office management. (Comment b, Sec. 757)

For a trade secret to receive the protection of law against unauthorized usurpers, it must be kept *secret*. Matters of public knowledge or general knowledge in an industry cannot be claimed as trade secrets, nor can information that is completely disclosed by the product itself. Trade secret protection will be lost if the owner discloses the information without protection; puts it on display; discloses it in trade circulars, technical publications, or photographs; or allows others to circulate it within the trade. In determining whether information should be granted trade secret status in an owner's suit to protect the information from exposure or to recover damages from exposure, a court will consider

> . . . (1) the extent to which the information is known outside of his business; (2) the extent to which it is known by employees and others involved in the business; (3) the extent of the measures taken by him to guard the secrecy of the information; (4) the value of the information to him and his competitors; (5) the amount of effort or money expended by him in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others. *Restatement*, Sec. 757, Comment b.

The owner must take reasonable precautions to keep the secret from being exposed to unauthorized persons but need not go to extreme and unduly expensive procedures to protect the information from flagrant industrial espionage [C-2].

If the owner has qualified the information as a trade secret, then his disclosure of the information to others under a confidential relationship or by contract, as with a controlled licensing arrangement, will be enforced by the courts under state laws. Anyone breaching the confidential relationship or violating the conditions of the license can be sued in court for tort or breach of contract [C-2].

Companies will often choose to protect valuable technical information as a trade secret rather than by means of a patent, either because the technology cannot meet the criteria to obtain a patent, or because they do not want their competitors to use the published information to "leapfrog" their technology to a more advanced product or process and thereby render their own item obsolete, or at least less valuable. This latter motivation is especially strong in those high-technology areas where technology is changing rapidly and a company must try to extend the life of its product technology in order to be able to recoup its costs in developing that technology.

THE SPARE PARTS AND COMPONENTS MARKET

According to industry sources, in many major industries incorporating advanced technologies (e.g., aircraft manufacturing), the companies that manufacture components for the final end product derive most of their profit from the sale of spare parts and services to support the item. For example, manufacturers of aircraft components such as wheel assemblies overwhelmingly make their profits in this "aftermarket," (i.e., sales and servicing that take place after the initial sale of the item). Very often, the competition for the sale of the original component is so stiff that little or no profit can be made on the initial item; all the profit in the item's life cycle is secured through the later supply of parts and support for the item. A good example is aircraft wheels and brakes. For these assemblies, the competition for the sale to the major aircraft assemblers is so severe that the suppliers essentially give them to the manufacturer in order to secure the business for the discs and other replacement parts and components supplied to the airlines that purchase the aircraft. This is much like giving away razors so that the razor maker will gain the recipient's future razorblade purchases. In such instances, the original manufacturer never

gives away the detailed technical data necessary for making the parts and components.

In contrast, in areas such as electronics, there is virtually no aftermarket for the original supplier, and all the profit must be made on the original sale. Another example is heat exchangers for aircraft. In these instances, there are many small contract manufacturers ("job shops") that can perform the repairs more cheaply than the original manufacturer because, among other things, they do not have to maintain an engineering staff. But to perform this function, these small companies must use the original manufacturer's technical data and thus must have the original manufacturer's cooperation.

How does a commercial buyer protect itself from exorbitant pricing by suppliers when the buyer is locked into a product with a long life and the supplier makes all or most of its profit from the sale of spare parts and support for the item? For example, how do airlines guard against price gouging in relation to brake discs and other supplier-unique wheel and brake replacement components when they have invested billions of dollars in a particular aircraft to which they are committed for many years? Normally, buyers will monitor what they are paying for spares and support and when they believe it has become excessive, they will protest to the supplier. If the supplier does not respond reasonably, the buyer will make sure that, in the future, that supplier is never included in another product it buys. A supplier that acquires a reputation for price gouging will soon have no customers.

How do the buyers know when spare parts prices are excessive? Usually, they simply compare the prices they are paying against the market prices for similar items on other aircraft. Also, contracts may contain provisions requiring the supplier to provide cost data on individual items as requested by the airline to satisfy it that the prices are reasonable.

Often in a major commercial or military program, the originator of a part or component will itself produce the item during the early phases of the program, when a large number of units are being produced. Later, as the production volume decreases (and perhaps as the technology becomes less sensitive to the source firm), the source may license another company that can produce the part more cheaply. The source firm receives a royalty from the licensee, the licensee gets the remaining production business, and the Government or other buyer gets a lower price.

REFERENCES

[C-1] James E. Hodder and Yael A. Ilan, "Technology Transfer and Second Sourcing When Production Costs Follow an Experience Curve," *IEEE Transactions on Engineering Management*, Vol. EM-34, No. 1, February 1987.

[C-2] Ralph C. Nash, Jr. and Leonard Rawicz, *Patents and Technical Data*, Washington, DC: The George Washington University, Government Contracts Program, 1983.

APPENDIX D

QUESTIONNAIRE ON RIGHTS IN TECHNICAL DATA

There continues to be conflict between the Department of Defense and its contractors and subcontractors over technical data rights issues. This survey is part of an information-gathering effort to help reduce that conflict. Your support in the survey will very significantly help in that effort. Please assist us with as many of the questions as you are able and willing to answer.

1. Company characteristics

a. Please briefly describe your company's primary business category (such as aerospace):

_____

_____

b. How large is your company in your business category?

_____ Large _____ Medium _____ Small

or

_____ Total annual sales (optional)

c. At what level (or levels) do you normally contract with DoD?

_____ Prime _____ Subcontractor _____ Subtier _____ Supplier

d. How much of your annual revenue is from DoD contracts or subcontracts?

_____ All or almost all _____ Most _____ Some _____ None

or

_____ Approximate percentage of annual revenue from DoD contracts or subcontracts (optional)

2. What data is "proprietary"?

The purpose of the following charts is to help define the circumstances in which contractors and subcontractors regard technical data as "proprietary" (see definition below). Please put an X in the boxes that would show how much data is proprietary in the different circumstances listed.

The following definitions apply to the chart:

- "Privately funded" means the product has been developed exclusively at private expense, with no part of the cost of development charged to a Government contract, whether development is for anticipated commercial or Government sale.
- "Product" means an item, component, part, or process.
- "Proprietary" means the technical data is "owned" by the company and no use should be made of the technical data without the express prior approval of the company. It does not necessarily imply that the company is very "sensitive" to the uses made of the data. For example, installation and operation manuals may be proprietary in the sense of being the exclusive property of the company, but the company may not be zealously protective about who gets to see or use the manuals.

CHART 1

PRIVATELY FUNDED PRODUCT DEVELOPED *PRIOR* TO GOVERNMENT CONTRACT OR SUBCONTRACT

		Type of modification to product made to satisfy DoD requirements				
		A major or minor modification is privately funded to meet DoD requirements	A *minor* mod is totally DoD-funded and the DoD and privately funded aspects *can* be segregated	A *minor* mod is totally DoD-funded and the DoD and privately funded aspects *cannot* be segregated	A *major* mod is totally DoD-funded and the DoD and privately funded aspects *can* be segregated	A *major* mod is totally DoD-funded and the DoD and privately funded aspects *cannot* be segregated
How much data is proprietary	All technical data for the whole end product (with modification) is proprietary					
	Only the privately funded data is proprietary					
	None of the end product data is proprietary					

CHART 2

PRODUCT DEVELOPED *DURING* THE COURSE OF A GOVERNMENT CONTRACT OR SUBCONTRACT

		Contractor funds part of product development and DoD- and company-funded aspects *can* be segregated	Contractor funds part of product development and DoD- and company-funded aspects *cannot* be segregated	Contract incorporates existing company-funded product into the end product and DoD/company-funded aspects *can* be segregated	Contract incorporates existing company-funded product into the end product and DoD/company-funded aspects *cannot* be segregated	Whole product is DoD-funded, but contractor contributes its technical know-how, engineering, and experience
How much data is proprietary	All technical data for the whole end product is proprietary					
	Only the privately funded data is proprietary					
	None of the data for the end product is proprietary					

Of course, the situations shown in the above charts do not describe all of the possible circumstances in which you might regard technical data as proprietary when it is developed or offered under a Government contract or subcontract. If there are any other proprietary circumstances which you feel are important and need to be highlighted, please list them below with a brief explanation.

3. For technical data you regard as proprietary (as defined above), please indicate in the chart below which combinations of data type and Government use you would strongly oppose. Put an X in any box where you would strongly oppose DoD's use of that specific kind of data for that specific purpose:

The following definitions apply to the chart:

- *Government uses of data* –
  - "Dual (alternative) sourcing" – the Government takes data your company has developed for a product (see above definition) and uses it to set up a second source of production as an alternative to your own company.
  - "Competitive reprocurement of spare parts and components" – after initial procurement of product from your company, DoD uses the technical data for the product to solicit the bids of alternative suppliers for spare parts and components of the product.
  - "Internal manufacturing" – the Government uses the data to manufacture the item in Government-owned facilities rather than a contractor's facilities.
- *Functional types or categories of technical data* –
  - "Detailed manufacturing or process data" – means technical data that describes the steps, sequences, and conditions of manufacturing, processing or assembly used by the manufacturer to produce a product or to perform a process.
  - "Detailed design data" – means technical data that describes the physical configuration and performance characteristics of a product in sufficient detail to ensure that a product produced in accordance with the technical data will be *essentially identical to the original product.*
  - "Form, fit, and function data" – means technical data that describes the required overall physical, functional, and performance characteristics, (along with the qualification requirements, if applicable) of a product to the extent necessary to permit identification of *physically and functionally interchangeable products.*

CHART 3

TYPES OF DATA AND DoD USES OF DATA

Types of data	Intended uses: Publication in public domain	Dual (alternative) sourcing	Competitive reprocurement	Internal manufacturing	Major overhaul	Routine maintenance	Installation and operation	Personnel training
Detailed manufacturing or process data								
Detailed design data								
Form, fit, and function data								
Installation, operation, and maintenance manuals								
Training manuals								
Preservation, packing, packaging, and marking data								

If there are any other combinations of types of data and DoD uses of that data which you would strongly oppose and that are not shown in this chart, please list those circumstances with a brief explanation:

_____

_____

_____

_____

4. Withholding technology.

a. As a result of concerns you have over loss or exposure of sensitive, proprietary data to your potential competitors under current DoD rules and practices, have you in the past withheld from a DoD procurement any of your best or latest technology?

_____ Yes _____ No

b. If your answer was yes, how frequently have you withheld – because of these data rights concerns – your best technology in the DoD procurements you participated in over the past five years?

_____ Always _____ Frequently _____ Rarely _____ Never

or

in approximately what percentage of DoD procurements that you participated in over the past five years did you refuse to include your best technology for this reason?

_____

c. If your answer in (a) was yes, do you think DoD was adversely affected because it did not receive your technology in its procurements?

_____ Yes, in all the procurements

_____ Yes, in some of the procurements

_____ No

d. Whether your answer in (a) was yes or no, do you expect to withhold your best technology from any future DoD procurements because of these data concerns?

_____ Yes _____ No

5. Nonparticipation in DoD procurements.

a. As a result of concerns you have over loss or exposure of sensitive, proprietary data to your potential competitors under current DoD rules and practices, have you in the past refused to participate in any DoD procurements or taken exception to the data rights requirements in the solicitation?

_____ Yes _____ No

b. If your answer was yes, how often over the past five years have you either refused to participate in DoD procurements or taken exception to DoD data rights requirements in solicitations?

_____ Often _____ Sometimes _____ Rarely _____ Never

c. Whether your answer was yes or no, do you think you will refuse to participate in any future DoD procurements because of these data concerns?

_____ Yes _____ No

6. Attrition.

a. Are you considering dropping out of the DoD market entirely?

_____ Yes _____ No

b. If your answer was yes, how strongly have data concerns influenced your decision, compared to other factors such as the declining DoD budget and number of programs?

0 ------- 1 ------- 2 ------- 3 ------- 4 ------- 5

No influence — Strong influence

c. Do you make privately funded investments in DoD-unique product improvement or development?

_____ Yes _____ No

d. If your answer was yes in (c) above, are you planning to reduce such investments in the future because of data concerns under current DoD rules and practices?

_____ Yes _____ No

7. Government Purpose License Rights certification.

a. When DoD conducts a competitive reprocurement of spare parts or components using the technical data of the original source in which DoD has Government Purpose License Rights, the bidders on the reprocurement are required to certify that they will use the technical data solely for that specific procurement and not for any other competitive business purpose or advantage. Do you believe this certification adequately protects your proprietary data from unauthorized use by such reprocurement bidders?

_____ Yes _____ No

b. If you answered no, is this DoD practice a major concern for you?

_____ Yes _____ No

c. To what degree would it help you if DoD were required to notify you anytime they release your Government Purpose License Rights data outside DoD (including the identification of the receiver(s) of the data)?

0 ------- 1 ------- 2 ------- 3 ------- 4 ------- 5

No help at all — Much help

8. Has your company experienced the unauthorized release (that is, a release violating current law or regulations) of its data being held by a military service?

_____ Yes _____ No

9. When your proprietary data is delivered to DoD and stored in a DoD data repository, how safe from unauthorized release do you believe your data is?

0 ------- 1 ------- 2 ------- 3 ------- 4 ------- 5

Not safe at all — Very safe

10. If you have concerns about the safety of your sensitive data in DoD possession, how much of an improvement would it be if the data were instead held in escrow by a neutral third party custodian?

-3 ------- -2 ------- -1 ------- 0 ------- 1 ------- 2 ------- 3

Much worse — No difference — Much better

11. If you have concerns about the safety of your sensitive data in DoD possession, how much of an improvement would it be if, all other aspects of the current DoD rules being unchanged, you were permitted to be sole custodian of that data until DoD called for it to meet an actual imminent need, rather than the current practice of ordering data for anticipated, but not-yet-occurring, needs?

0 ------- 1 ------- 2 ------- 3 ------- 4 ------- 5

No better — Much better

12. How significant an improvement over the current DoD rules and practices would it be if you were only required to deliver form, fit, and function data instead of more detailed product data?

0 ------- 1 ------- 2 ------- 3 ------- 4 ------- 5

Not significant — Very significant

13. In your company's DoD contracting experience, has DoD ever – using its superior bargaining position – insisted on taking more rights in your data than are normally permitted under the regulations?

_____ Never _____ Rarely _____ Sometimes _____ Often

14. In selling to commercial companies, has your company ever been required, as a non-negotiable condition of the contract, to deliver proprietary technical data that could possibly be used to establish an alternative source (either for an item, spare part or component, or process) for the buyer?

_____ Never _____ Rarely _____ Sometimes _____ Often

15. In buying from other commercial companies, has your company ever successfully insisted on acquiring proprietary technical data from a supplier?

_____ Never _____ Rarely _____ Sometimes _____ Often

APPENDIX E

GLOSSARY

ASPR	=	Armed Services Procurement Regulation
CAD	=	computer-aided design
CALS	=	Computer-aided Acquisition and Logistic Support
CAM	=	computer-aided manufacturing
CDRL	=	Contract Data Requirements List
CICA	=	Competition in Contracting Act
CITIS	=	Contractor Integrated Technical Information Service
DFARS	=	Defense FAR Supplement
DID	=	data item description
DoDI	=	DoD Instruction
FAR	=	Federal Acquisition Regulation
GAO	=	General Accounting Office
IG	=	Inspector General
GPLR	=	Government purpose license rights
ILS	=	integrated logistics support
IR&D	=	independent research and development
IWSDB	=	Integrated Weapon System Data Base
LMI	=	Logistics Management Institute
NDI	=	nondevelopmental item
P.L.	=	Public Law
TDP	=	technical data package
U.S.C.	=	United States Code